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.

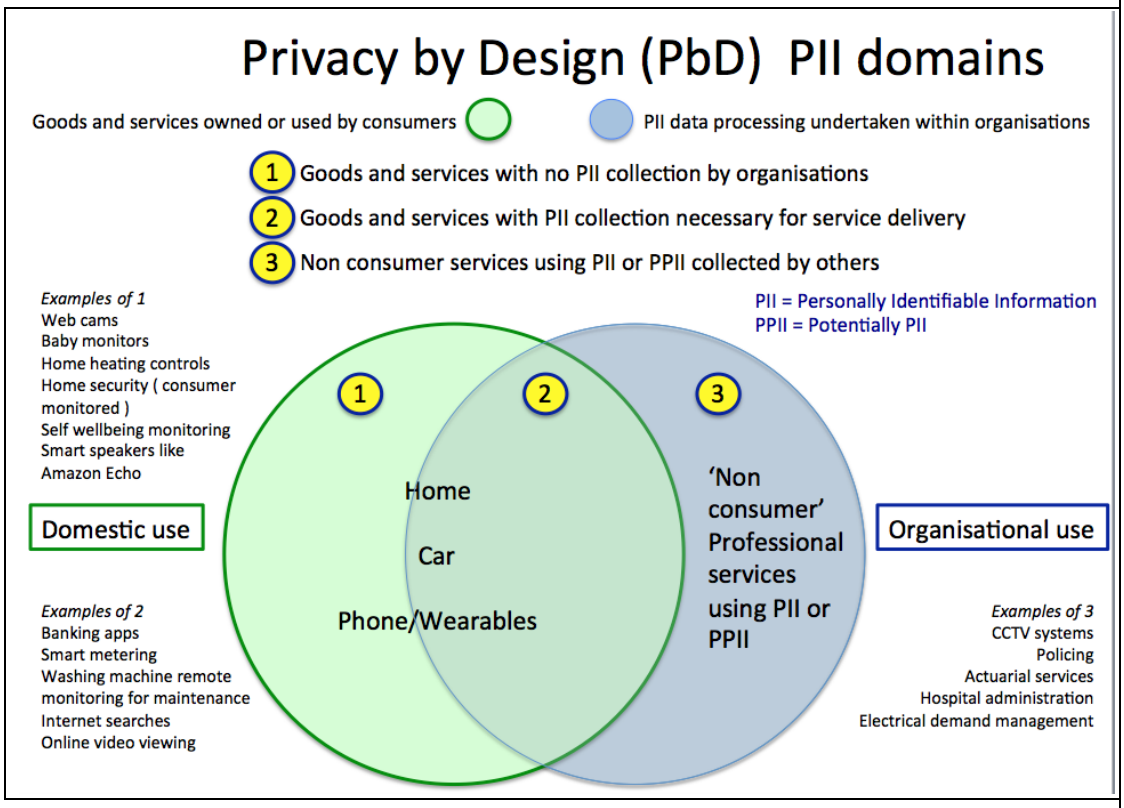
☒ Annex(es) are included with this proposal (give details)

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 :-

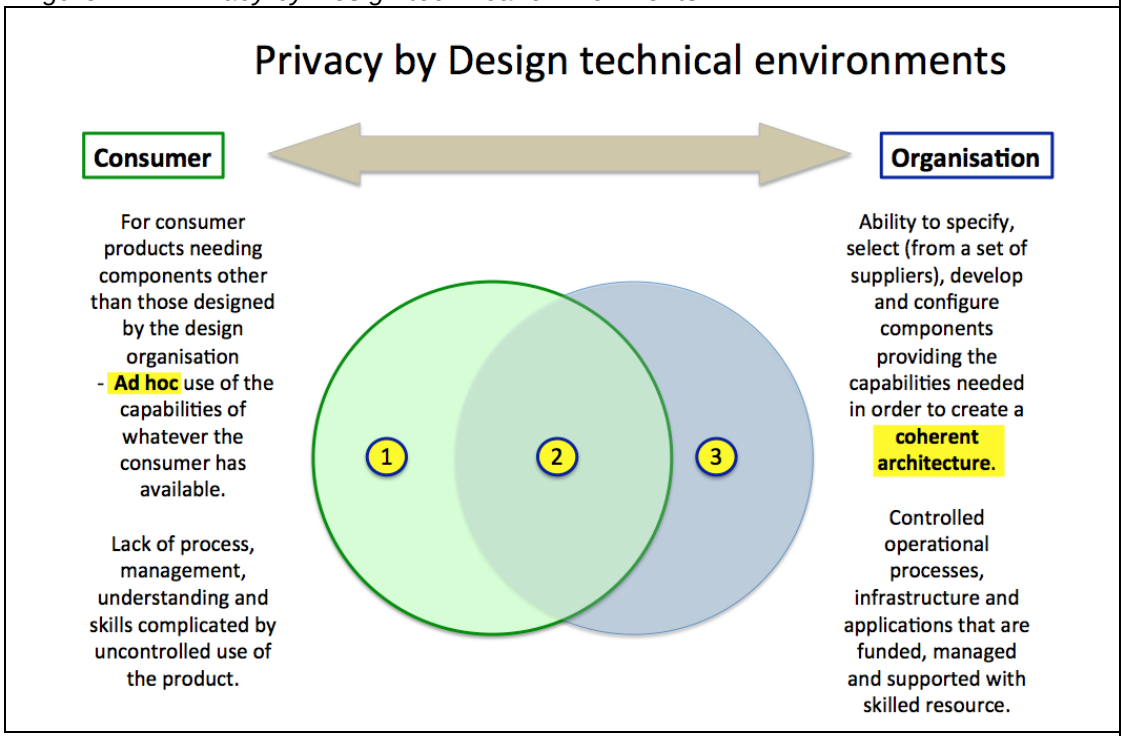
- data passed on from original PII collection that meet the original purpose for that collection

- 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.

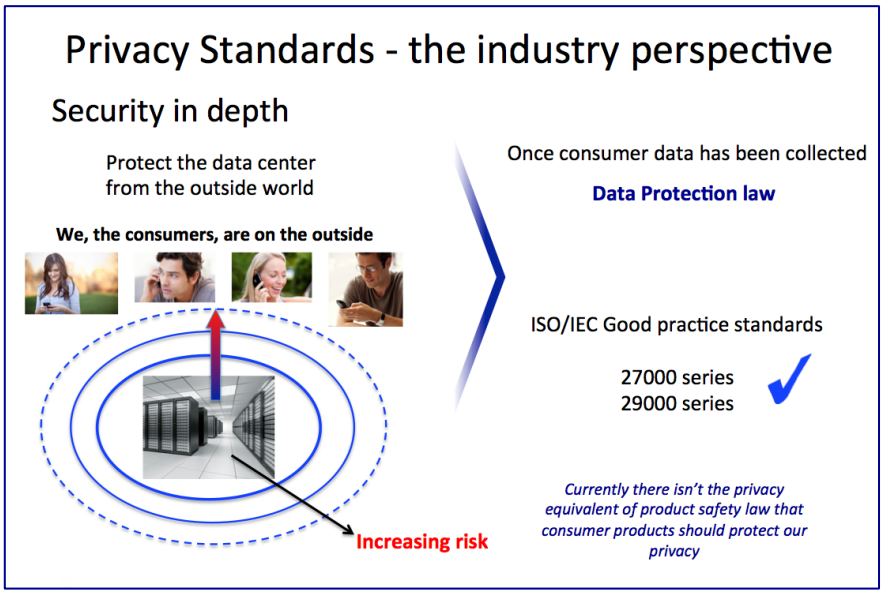
These are two very different design environments with different requirements and risks to be addressed through design.

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

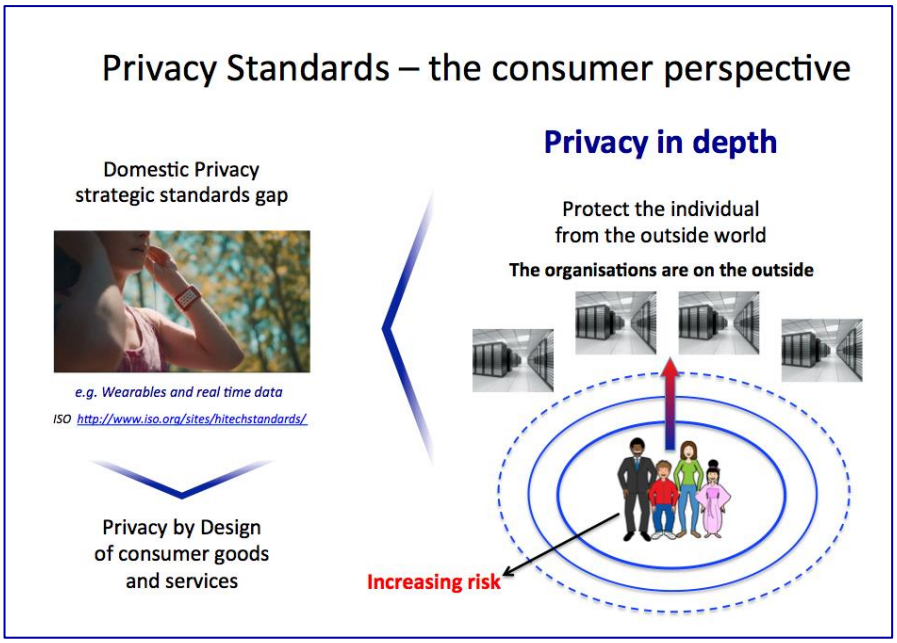
The current JTC 1 Security and Privacy standards address domain 3 and a number of aspects of domain 2 with their organization centric approach. The Industry perspective is illustrated in figure A1.3

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.

List of potential sections in a consumer protection standard for privacy by design of consumer goods and services

Left blank

Foreword – *to be developed*

0. Introduction

0.1 Background and context

Designing for consumers

Designing products that are used in the consumer domestic domain is very different from designing for an organization. Consumers are very low on understanding the technology, unskilled, unmanaged, with no formal processes, have significant human vulnerabilities and limited capabilities that can be exploited, and consumers can use products in unexpected ways.

This means that consumer goods and services design faces significantly different challenges compared to the design of managed corporate infrastructures, systems and applications. For this reason the approach of this standard is to emphasize consumer protection through technical solutions incorporated directly into consumer product design thereby reducing the need for human dependent protective actions.

System design for organizations' managed infrastructures utilizes selected and configured components to ensure coherence of technical security and privacy controls together with processes to administer and monitor the effectiveness of their implementation. In the consumer domestic environment designers face a different challenge of "loose" integration through design for interworking with ad hoc sets of 3rd party products purchased or used by consumers. Consequently 3rd party software and hardware components such as routers and mobile phones are integral to the environments in which consumer products are operated, and so the role of such 3rd party products is addressed in the standard's design process.

Relationship to other standards

This International Standard provides requirements derived from ISO 10377**:**2013 "Consumer product safety -- Guidelines for suppliers" and many ISO/IEC JTC 1 standards and study reports. The standard addresses consumer protection through a design process for consumer goods and services to meet consumer privacy needs. The standard adapts and focuses ISO 10377:2013 and the existing JTC 1 standards relevant to consumer privacy and applies the continuous improvement cycle of ISO 9001.

The standard addresses a key gap in the ISO/IEC 29100 framework and associated standards. Whereas ISO/IEC 29100 is organisation and data protection focused it explicitly excludes consumer domestic processing purposes. Such domestic use privacy control is missing from ISO/IEC 29100 considerations. This standard addresses within family and friends privacy controls when processing is for personal purposes. It should be noted that approximately 30% of consumer privacy needs are for those required for domestic privacy.

The aim is to provide consumer and human centered privacy by design that specifically applies to the way that products are used by consumers and the associated privacy design factors.

The standard allows product (ie goods and services) designers and providers to demonstrate, through compliance, consumer protection, especially for children's use of products, fulfilling the need to protect consumers from fraud, exploitation of their data, cyber bullying, ransom demands, and other forms of privacy invasion and privacy breaking exploits resulting from lost and stolen personal data.

Security of domestic devices

Consumer domestic privacy is scoped to include the security of devices and processing in the domestic environment so that this aspect is also addressed within this standard.

In addition the standard has been scoped to address the nature of software and the need for a significant number of in life software design updates to products, especially for security in order to meet the latest threats and exploits.

Given the role of consumer digitally connected devices in increasing the global cyber attack surface and consumer devices being used by hackers to threaten organisations' operational and security infrastructures, the standard makes a key contribution to cyber security too helping to protect from the sequestration of consumer devices.

Regulation

Where users of the standard wish to address local or regional data protection regulation the structure supports the incorporation of such regulatory requirements to ensure that the developed products comply with the desired data protection regime.

0.2 Understanding consumers

Privacy considerations for the use of Consumer goods and services are addressed through use case methodologies covering normal and foreseeable use, un-anticipated and foreseeable unintended uses, as well as foreseeable active misuse.

The detailed requirements for privacy controls and product security are are applicable to personal wearable and portable products, personal transport products and domestic dwellings and are based on several basic requirements:

a) Consumers need their products to be inherently secure
b) Consumers need high levels of domestic privacy control to allow them to adjust sharing with other consumers and data collection consents for organisations in real time to match the individual privacy contexts where they wish to exercise privacy control.
c) Consumers expect that, once their personal data has been collected by an organization, the processing of that data shall protect their privacy.
d) Consumers expect transparency of use of their data when passed, traded, swapped or moved between 3rd parties so that they can ascertain who is

processing their data and for what purposes in order to be able to exercise their rights for visibility, correction and removal under data protection law.

e) Design that addresses consumer human capabilities and vulnerabilities
f) As a base, design that addresses the legal and regulatory requirements with respect to data protection to be applied according to the jurisdictions in which data processing is undertaken.

0.3 Information privacy control and security requirements

It is essential that consumer product designers identify the privacy control and security requirements relevant to consumers' needs. The main means of deriving privacy control and security requirements are:

a) The product definition of features, functionality, facilities, performance and the consumer privacy needs, as well as objectives and business requirements placed on information processing that have been developed by the organization for supporting its business operations.

b) Use cases
For the privacy by design process for consumer products use cases play an essential role in

- identifying any privacy risks and managing them,
- identifying and implementing risk reduction measures,
- implementing processes and incorporating design features that support product identification and trace-ability for upgrade and corrective actions,
- communicating use and warning information to consumers,
- monitoring the product in the market place

c) Software and hardware security design good practices

d) The results of consumer product design Privacy Impact Assessment

e) The requirements that result from legislation and bye-laws, regulations and contracts which have to be fulfilled by an organization, and sociocultural requirements.

0.4 Design to meet privacy control and security requirements

Once the privacy control and security requirements and risks have been identified and decisions taken on how to deal with the risks, detailed design is then undertaken to implement the requirements through development of the target consumer equipment and any organizational application software contributing to the product functionality.

In addition design needs to incorporate features, functions and facilities to maintain and upgrade as necessary those privacy controls and security features for an environment that is under constant threat with continually evolving exploitation actions by malicious parties.

It has been recognized that practical design methodologies may iterate a number of times during the design process.

0.5 Audience

This International Standard provides practical requirements for product developers and suppliers of all sizes to enable them to demonstrate good practice in privacy by design for the consumer products they supply. Good practice includes the design and testing of the product, design using components and other products utilized to deliver the product functionality, production, distribution to consumers and product consumer use and disposal.

This International Standard is intended to be practical for small and medium sized organizations as well as enterprises undertaking consumer product development and supply.

This International Standard does not cover issues such as worker privacy or wider social and ethical issues as the standard focuses on consumer products and the very different environment in which they are used.

1. Scope

1.1 This International Standard provides a set of requirements to be met by those undertaking privacy by design and provision of consumer goods and services that allow demonstration of good design process practice for privacy by design in order to increase consumer confidence when purchasing goods or being asked to use goods and services for their domestic activities.

1.2 The design process scope includes consumers' domestic processing privacy needs as well as the privacy requirements of Data Protection.

1.3 The functional scope includes product security in order to prevent unauthorised access to data as fundamental to consumer privacy, and consumer privacy control with respect to access to a person's data and their authorization to use that data for specific purposes.

1.4 This International Standard applies to

- any domestic equipment (i.e. hardware and software) provided to consumers whether that equipment is used for only domestic purposes or both domestic and organisational purposes
- any organisational terminal equipment and application software that undertakes functions necessary to provide the consumer with the product capabilities intended by the design and whether that functionality is provided within an organisation's systems and infrastructure or the application software processed on 3rd party services.

2 Normative references

to be agreed

3 Terms and definitions

To be determined

4 Symbols and abbreviated terms

to be developed

5 – Understanding the role of consumers

5.1. General

In order to understand consumer decisions and actions that may have a significant impact on whether or not the product causes privacy harm providers of a consumer good or service shall demonstrate that they understand real consumer behaviour during purchasing, assembling/installing, using, storing, maintaining and disposing of consumer goods and services.

Providers of a consumer good or service shall demonstrate that they have provided product information to consumers that will enable consumers to make informed decisions when purchasing or choosing to use a consumer good or service and to behave in a privacy safe manner in using and disposing of the product.

5.2. Pre-purchase

Providers of a product shall provide information to consumers on the privacy features of the consumer product which may include labelling or advertising that addresses product use. Such information shall when consumers may be at privacy risk when using the product and specific high risk actions.

5.3. Use

Instructions for assembly and privacy configuration, intended and privacy safe use, maintenance, storage, lifespan and disposal shall be provided to consumers.

The means chosen to make this information initially available to consumers shall not depend on the product being digitally connected. Subsequent updating such information may make use of networked capabilities.

Text and diagrams shall be readable, clear and easy to understand.

If product privacy assistance may be needed at some time, then product providers shall identify that such assistance may be required, how to access that assistance and ensure that such assistance is available.

If product privacy professional maintenance may be needed at some time, then product providers shall identify that such assistance may be required, how to access that assistance and ensure that such assistance is available.

Product providers shall maintain a goods recall database and or service withdrawal data base so that those consumers affected by product recall or service withdrawal can be contacted and informed of associated consumer action that may be needed.

5.4. Feedback from consumers

Product providers shall obtain information from consumers about their use of the consumer product.

Such feedback may include :

- Consumer feedback during product marketing
- Consumer complaints and privacy issues provided to the product provider
- Consumer reports made to regulatory bodies
- Consumer information provided during claims and lawsuits

Consumer information shall be catalogued and fed into the use case definition and specification in the privacy by design process to feed into any further iterations of the product design.

Product providers shall provide consumers with information on how to report incidents and how to detect potential privacy hazards

5.5. Vulnerable consumers

If the product is to be used by consumers with less than average capabilities or who may have vulnerabilities that inhibit their ability to understand and exercise control over their privacy or to provide feedback about their product use then product providers shall consult with government officials and civil society groups to help provide a means for supporting their privacy needs and providing feedback about their product use.

6. Consumer goods and services design concept model

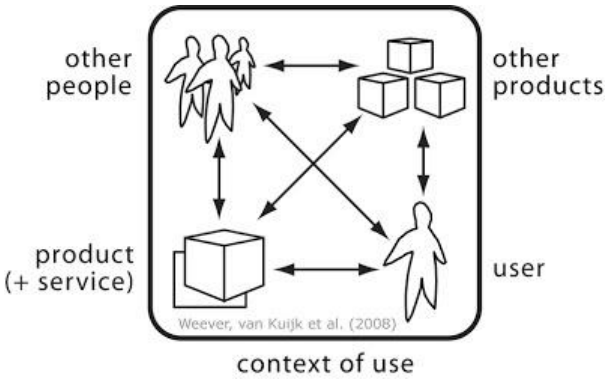
6.1. The basis of the model

The consumer product privacy design concept model addresses the domestic domain and the organization domain as scoped in section 1.4.

The concept model includes 3rd party products needed in both domestic and organizational domains for the product to function.

The model uses an extension to Shackel's framework for human-computer interaction as developed for networked products by Renee Wevera⁎, Jasper van Kuijkb and Casper Boksc 2008[1].

Figure 1 Model for products functioning in networks



The framework of figure 1 of users and products is applied twice; once in the consumer domain and once in the organizational domain. These two domains are connected by communication services.

[1] *International Journal of Sustainable Engineering Vol. 1, No. 1, 2008*
User-centred Design for sustainable Behaviour
Renee Wevera⁎, Jasper van Kuijkb and Casper Boksc

6.2. The roles of users

6.2.1 Consumers

In the domestic domain, a role of primary user is assigned to the consumer as the person whose personally identifiable information is being processed.

The model allows for other consumer users as responsible 3rd parties such as parents and carers, as well as other consumers as friends and family users when for example pictures are shared or local friends help 'look after' a house, while the family is away, by participating in digital surveillance of the house's cameras and security sensors.

6.2.2. Organisational users

Where the consumer product interacts with an organization for the purposes of service provision the model allows for the identification of different roles for those organizational users who have access to or participate in the processing of the consumer's data. For example, field maintenance service technicians, complaints handling officers, product research managers and so on.

6.3. 3rd party products

The model also incorporates 3rd party products to enable the design process to address the design issues of the product needing to interwork with other products to provide all the functionality intended for the product.

For the domestic domain, such 3rd party products are treated differently in the design process as designers can only make use of the existing ad hoc security and privacy capabilities of 3rd party products for their own product design.

3rd party products used in the organizational domain may be closely specified so that there is tighter control over the design and interworking requirements. However, the means adopted in the standard for the domestic domain 3rd party products may be applied to the organizational domain where designers find they do not have control over the 3rd party product specification and have instead to make use of what has been implemented by the organisation.

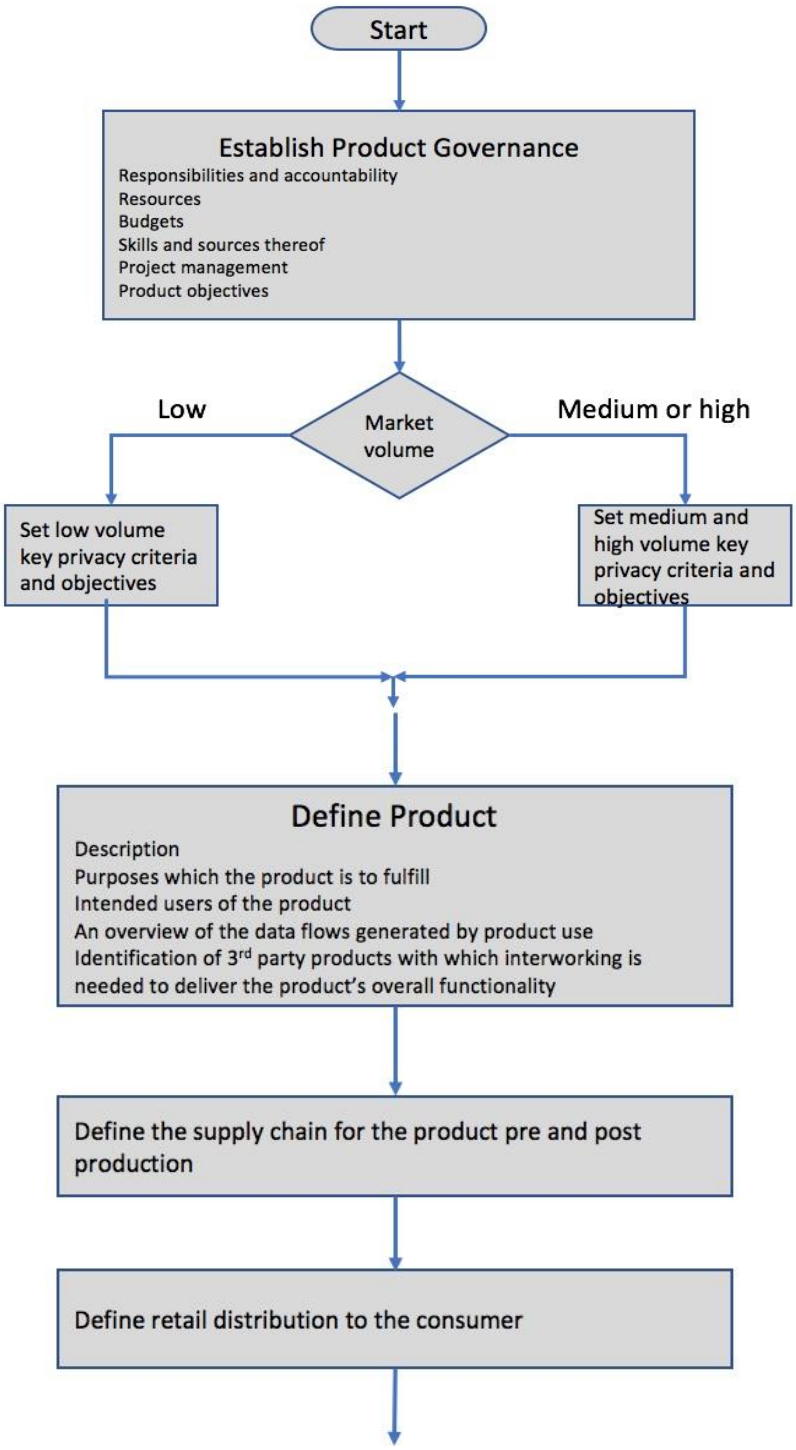
7. The consumer product privacy by design process overview

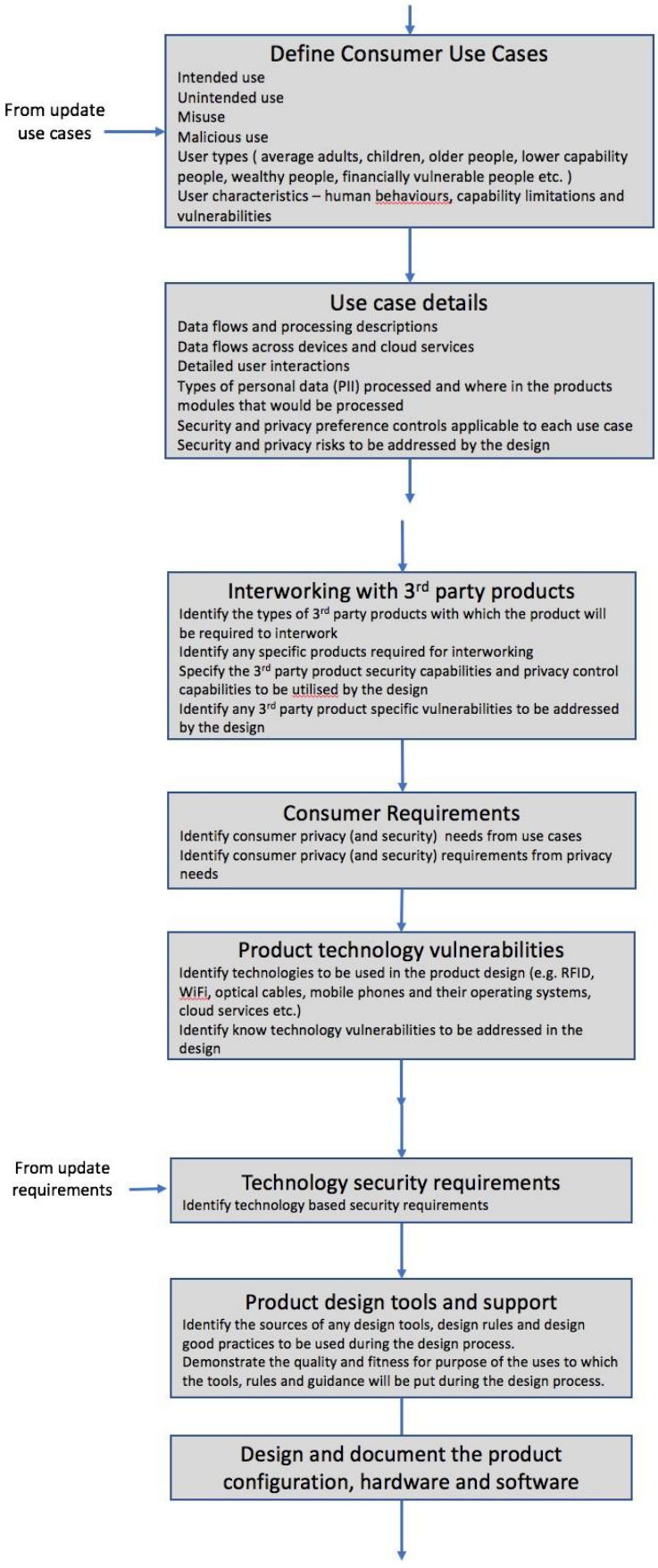
The privacy by design process for consumer goods and services progresses through a number of steps as follows :-

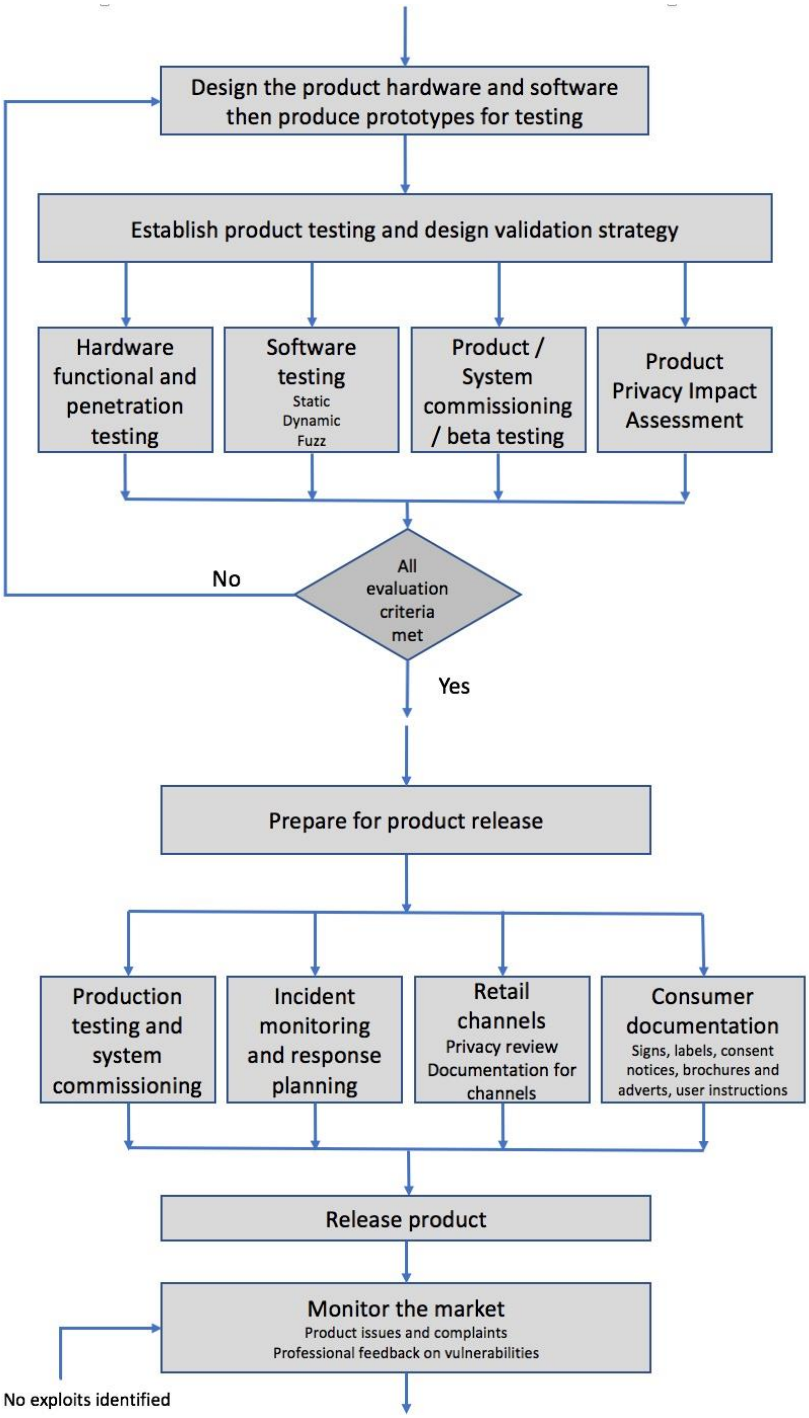
- Defining the product and setting its context
- Understanding consumers and the consumer context
- Product technology and security requirements
- Designing the product and producing prototypes
- Product testing and design validation
- Preparation for product release
- Monitoring the market and taking remedial action when needed
- Maintaining product privacy at end of lifecycle

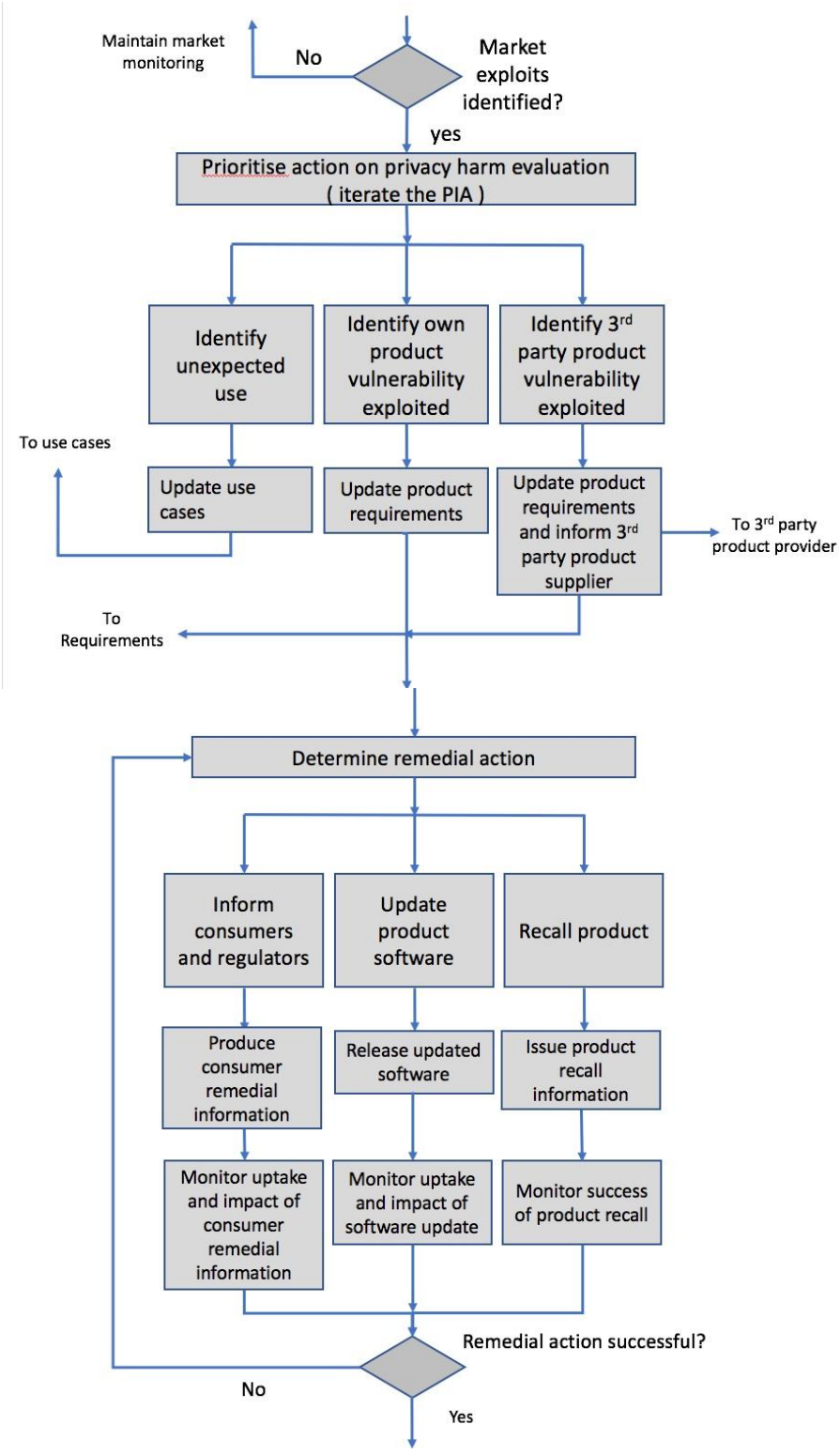
8. Privacy by Design of Consumer Goods and Services - Process flow overview

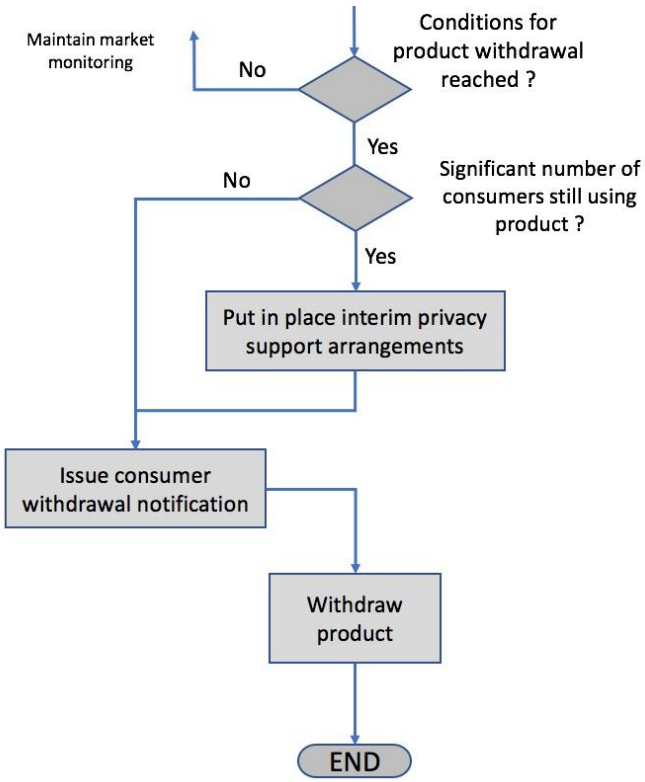
The following flow diagram provides an overview of the logic of the process, the key decision points and feedback paths needed for privacy by design.




From update use cases
Define Consumer Use Cases
Intended use
Unintended use
Misuse
Malicious use
User types (average adults, children, older people, lower capability people, wealthy people, financially vulnerable people etc.)
User characteristics – human behaviours, capability limitations and vulnerabilities
Use case details
Data flows and processing descriptions
Data flows across devices and cloud services
Detailed user interactions
Types of personal data (PII) processed and where in the products modules that would be processed
Security and privacy preference controls applicable to each use case
Security and privacy risks to be addressed by the design
Interworking with 3rd party products
Identify the types of 3rd party products with which the product will be required to interwork
Identify any specific products required for interworking
Specify the 3rd party product security capabilities and privacy control capabilities to be utilised by the design
Identify any 3rd party product specific vulnerabilities to be addressed by the design
Consumer Requirements
Identify consumer privacy (and security) needs from use cases
Identify consumer privacy (and security) requirements from privacy needs
Product technology vulnerabilities
Identify technologies to be used in the product design (e.g. RFID, WiFi, optical cables, mobile phones and their operating systems, cloud services etc.)
Identify know technology vulnerabilities to be addressed in the design
From update requirements
Technology security requirements
Identify technology based security requirements
Product design tools and support
Identify the sources of any design tools, design rules and design good practices to be used during the design process.
Demonstrate the quality and fitness for purpose of the uses to which the tools, rules and guidance will be put during the design process.
Design and document the product configuration, hardware and software


Design the product hardware and software then produce prototypes for testing
Establish product testing and design validation strategy
Hardware functional and penetration testing
Software testing
Static
Dynamic
Fuzz
Product / System commissioning / beta testing
Product Privacy Impact Assessment
All evaluation criteria met
No
Yes
Prepare for product release
Production testing and system commissioning
Incident monitoring and response planning
Retail channels
Privacy review
Documentation for channels
Consumer documentation
Signs, labels, consent notices, brochures and adverts, user instructions
Release product
Monitor the market
Product issues and complaints
Professional feedback on vulnerabilities
No exploits identified


Maintain market monitoring
No
Market exploits identified?
yes
Prioritise action on privacy harm evaluation (iterate the PIA)
Identify unexpected use
Identify own product vulnerability exploited
Identify 3rd party product vulnerability exploited
To use cases
Update use cases
Update product requirements
Update product requirements and inform 3rd party product supplier
To 3rd party product provider
To Requirements
Determine remedial action
Inform consumers and regulators
Update product software
Recall product
Produce consumer remedial information
Release updated software
Issue product recall information
Monitor uptake and impact of consumer remedial information
Monitor uptake and impact of software update
Monitor success of product recall
Remedial action successful?
No
Yes


Maintain market monitoring
No
Conditions for product withdrawal reached ?
Yes
No
Significant number of consumers still using product ?
Yes
Put in place interim privacy support arrangements
Issue consumer withdrawal notification
Withdraw product
END

9. Product Privacy by Design Governance

For the purpose of ensuring that the right governance arrangements are in place for privacy by design organizations shall as a minimum specify:

9.1. Responsibilities and accountability

9.1.1. Responsibility for overview of key privacy criteria set for the product and business decisions affecting privacy shall be assigned to a senior business manager with responsibility for

- Managing stakeholder engagement for the product
- Establishing the balance between consumer and public interests and organisational or commercial interests
- Authorizing key privacy objectives set and any changes of these for the product
- For SME and Innovation practices - Authorizing any low market volume process where rapid development and testing are to be supplemented by early product release requiring good market monitoring to be in place for capture of user issues with the product, combined with agile problem resolution for users.

9.1.2. Responsibility for product privacy design shall be assigned to a senior member of the design team with responsibility for

- use cases used to determine privacy needs
- security and privacy controls requirements set for the product
- reviewing privacy performance and PIA evaluation information
- consumer, retailer and regulator privacy information provision
- 3rd party product security and privacy controls information provision to the design team
- provision of product and 3rd party product vulnerabilities and exploits information to 3rd party product providers

9.2. Resources

9.2.1. A senior business manager shall be responsible for the product budget and provision of internal and external resources necessary to undertake the privacy by design process specified in this standard.

9.2.2. The product team leader shall provide statements of the skills, tools and capabilities to be used for the development, manufacturing and post release phases of the product.

9.3. Product development project management

9.3.1 The product team shall include a project management with responsibility for development activities.

9.3.2. The project manager shall publish and maintain a project plan that demonstrates how the resources applied to the product development delivers the key privacy objectives set for the product.

9.4 Key privacy design criteria

9.4.1. The design team leader shall provide product design privacy performance criteria for release of the design to production including

- privacy impact assessment results
- software testing
- hardware penetration testing
- product/system testing / beta testing results

9.4.2. The senior manager responsible for the product's privacy shall review and may authorize the release of the product to market when the product meets the privacy objectives set for product release.

9.4.3. The senior business manager with responsibility for the product privacy shall ensure that assessment criteria for product release to the market are available including:

- Production testing and system commissioning for product release to the market
- Readiness of market monitoring for receiving product vulnerability and privacy issues
- Retail channel privacy reviews, privacy information to and briefing of channels
- Readiness of consumer privacy documentation
- Privacy harm levels that trigger product design changes
- Readiness of online update processes and capabilities
- Readiness of product recall processes and capabilities
- Readiness of remedial action processes
- Regulator information provision

9.4.4. The senior business manager with responsibility for the product privacy shall authorize assessment criteria for product withdrawal

10. Records

10.1. Pre product release records and document control
– technical reference see pages 7 and 8 of ISO 10377

Documentation and records shall be provided that reflect privacy by design for development, production and the market place. Such records may include:

i. records arising from the implementation of this International Standard
ii. records required to comply with laws and regulations
iii. documents created during the design process such as
- use cases employed for design and privacy impact assessment

- hazard analysis and risk reduction plan
- significant design choices and privacy decisions
- privacy impact assessments and PIA summaries

iv. drawings, product specifications and copies of digital code
v. product security and privacy capability statements for use by other product developers
vi. product quality tests and sample products
vii. design validation documents
viii. warnings and instructions for consumers and users
x. design testing and inspection
x. cost benefit analysis of corrective actions
xi. compliance with regulatory requirements and product specify industry standards
xii. 3rd party testing and conformity assessment capabilities used
xiii. 3rd party product privacy and security capabilities used of the 3rd party products to be deployed in the domestic environment where interworking is needed to provide the overall designed product functionality
xiv. 3rd party tools and services used to assist the design process; what used, quality and validation of source of the tools/services

10.2. Post release of product records for privacy monitoring and privacy issue resolution

i. post market release privacy checks, audits and testing
ii. consumer complaints and privacy incidents, and vulnerability and exploit reports from professional
iii. records from the sale and distribution of products throughout the supply chain
iv. product literature including advertising marketing and packaging
v. communications with suppliers and consumers including product registration post-sale warnings, market surveys and feedback form sales and distribution channels
vi. reasons for returned products and service records
vii. corrective actions including online software updates, firmware re-issuing, instructions to sales and distribution channels

11. Product Definition

For the purpose of providing sufficient understanding of the consumer for product privacy design to proceed the following shall be provided as a minimum:

a) a product description
b) identification of the intended users of the product
c) a description of the purposes that the product fulfils for consumers
d) a description of the purposes that the product fulfils for the organisation
e) a description of the functions features and facilities provided by the product

f) a description of the physical form of the product and the way that users interact with the product
g) a description of the data processing purposes undertaken by the product
h) an overview of the data flows generated by product use
i) a description of the other products where interworking is needed to provide overall product functionality

12. Supply chain and retail definition

The senior business manager responsible for product privacy governance shall, for for the purposes of privacy design define the supply chain, retail activities and channels, access channels and support arrangements for the product.

12.1 Component sourcing

The design team shall identify as a minimum :

a) hardware and software components brought in for use in the product design
b) the organisations sourcing those components
c) the privacy and security checks on components undertaken in order to incorporate the components into the design.
d) any privacy issues associated with components
Technical note: for example unique chip id codes on RFID chips have privacy implications. *Hardware and software components may come with known security vulnerabilities*

12.2 Product distribution

For product distribution to consumers as a minimum for privacy by design purposes the following shall be identified:

a) The supply chains used to bring the product to online or physical retail outlets
b) Any privacy issues associated with those supply chains
Technical note: for example warehouse tampering with products and for software distribution server hacking or embedding of malware

12.3. Online and Retail outlets for consumers

For product distribution to consumers as a minimum for privacy by design purposes the following shall be identified:

a) The online and retail outlets used to make the product available to consumers
b) Any privacy issues associated with those online and retail outlets
Technical note: for example apps (for smart phones) made available via a company's own web site has associated privacy

risks of scam e mails mimicking the vendor and routing consumers to fake webs sites to download malware. This is one reason why in the UK OFCOM recommends apps be only made available via the phone associated apps store.

13. Use case definition for consumers and other users

13.1. General

Product providers shall have an understanding and knowledge of the consumer product's uses and knowledge of how it will actually be used.

If the product design process is to make use of the criteria for low market volumes suitable for SME's and innovation projects then product providers shall have in place rapid feedback and agile change processes in place in order to rapidly build up knowledge and understanding of product use.

Product use shall be reviewed and updated when feedback from development testing or the market place shows that unanticipated use is creating privacy risk levels exceeding tfhe criteria set for the product.

Use cases shall be defined for

a) foreseeable use
b) foreseeable misuse
c) foreseeable malicious use

13.2. Foreseeable use

Consumer product providers shall have knowledge of foreseeable product use. Such knowledge may be derived from sources such as :

- use consistent with its function and design including technical data on the function and design of the product
- use of a product based on factual human behaviour and physical characteristics
- use of a product associated with meeting the regulatory requirements of the judicial domains applicable to the product (such as use cases for personal data access and correction)
- use of a product based on consumer feedback
- use of a product based on the institutional knowledge of the provider
- use of the product that is consistent with the law and regulations in the locations where the product is used, and the product data is processed
- use of the product consistent with industry knowledge of that particular product or products of that type.

13.3. Foreseeable misuse

Consumer product providers shall have knowledge of foreseeable product misuse. Such knowledge may be derived from sources such as :

- the use of a product based on factual human behaviour or measurements
- the use of a product based on feedback from consumers, voluntary and professional bodies

- demographics information from marketing and consumer trends
- use of the product based on the institutional knowledge of the provider
- use of the product consistent with industry knowledge of that particular product or products of that type.
- reports of failure caused by the consumer improperly assembling, installing maintaining and caring for the product

13.4 Foreseeable malicious use

Consumer product providers shall have knowledge of foreseeable product malicious use. Such knowledge may be derived from sources such as :

- security and privacy experts' information on malicious use
- known design rules to mitigate malicious use
- use of the product based on the institutional knowledge of the provider
- use of the product consistent with industry knowledge of that particular product or products of that type. Particular attention may be paid to known hacks that have effective rapid distribution and activation mechanisms.
- consumer reports and feedback on privacy incidents
- consideration of actions that break regulatory guidance and requirements
- civil society organisations information on scams and other forms of consumer harm derived from use of the product

13.5. Unforeseeable uses of all types

The product provider shall establish mechanisms to receive feedback from the market place regarding product uses. This feedback shall be monitored and analysed to identify repeatable patterns.

13.6. Other types of use case

Product providers may include use cases for :

- Use by different consumer user types such as average adults, children, older people, lower physical and mental capability people, wealthy people, financially vulnerable people etc.
- Use by different organizational user types with different roles and responsibilities
- Use of the product for cyber bullying and abuse
- Use of the product to effect scams
- Loss of PII held within the organisation
- Retail channels selling and misuse
- Product servicing
- Product online update
- Product re-call
- Problems with 3rd party product design updates
- Product loss or theft
- Change of consumer ownership passing the product on to others such as private sales, second hand markets and car boot sales, charity shops, gifts etc.
- Change of product provider ownership with differing privacy policies and terms and conditions to be applied
- Product provider bankruptcy
- Changes to regulations

13.7. Use case review and update

Use cases shall be reviewed, updated and cases added as design details, privacy impact assessments, product penetration testing, market feedback and other information relevant to product use that varies from current use cases becomes available to the product provider.

13.8. Use cases for product privacy design

The use cases for which design is to be undertaken shall be identified and kept up to date as the design process proceeds.

13.9. Use cases for product privacy evaluation

The use cases for which privacy impact assessment and penetration testing shall be undertaken shall be identified and kept up to date as the design proceeds.

13.10. User identification in use cases

Each use case shall identify

a) the primary human user for that case
b) what the primary human user is intending to achieve through intended use
c) other human users involved in the use case, including other consumers (such as children), organizational users and malicious users.
d) any intended human users having capability limitations
e) known human user privacy vulnerabilities and behaviors
f) factors affecting consumer exposure to risks such as frequency of operation, use of radio technology, accessing web sites with poor malware protection, consumer time spent in public spaces with the product
g) any automated entities taking part in the processing for the use case

13.11. Privacy context for use cases

Each use case shall define the privacy context applicable. The privacy contexts may include:

a) domestic only use
b) mixed domestic and organizational use
c) social sharing
d) public environments (for example walking down the road and using an app on a smartphone to find a restaurant to eat at or to book a taxi)
e) any other privacy contexts not addressed by a), b), c), or d)

(Technical note: This context definition requirement assists in identifying relevant privacy needs)

13.12. Identification of interworking with 3rd party products and systems

Descriptions shall be provided of any other products or systems that play a role in providing the functionality needed for product use in each use case.

13.13. Use case stakeholders and their interests

Stakeholders shall be listed
Stakeholder interests shall be listed for each stakeholder

13.14. Use case descriptions

Each use case definition shall describe

a) how the product, as defined in section 11, is used by each user identified.

b) how each of the users interact with the product to achieve their aims in using the product.

c) The consumer privacy needs to be met by product design.

d) The necessary communication between product modules and with 3rd party products shall be described for the user interactions and for functions that the product needs to undertake for each interaction,

14. Use case specification

14.1 Each use case shall specify:

a) Detailed user interactions
b) Data flows and processing descriptions
c) Data flows across devices and cloud services
Technical note: this may utilise good practices from ISO/IEC 19944 Data flows across devices and cloud services.
d) Types of personal data (PII) processed and where in the products modules that would be processed
e) Privacy preference and security controls applicable to each use case

14.2. Product Interaction Specification

In order to provide detailed user interactions for 14.1 (a) the purpose of the interaction and the manner of the interaction (e.g. voice / touch screen etc.) shall be provided for any interactions between the product and the following:

a) with users
b) with other domestic products
c) with product provider applications processed on that provider's infrastructure

d) with 3rd party products and services interacted with by product provider applications processed on that 3rd party's infrastructure and not in the domestic environment.
Technical note: for example credit check services undertaken by 3rd parties for credit providers

14. 3. PII Data Specification

For each use case the PII processed shall be specified for the following PII processes:

a) PII input by users
b) PII input from 3rd party products (e.g. smart meters into home energy budget running as an application on a home PC)
c) PII created or processed by the product within the domestic equipment
d) PII created or processed by the product provider's applications (processed on that provider's infrastructure) where PII is collected, created, stored, used, shared, transmitted, transferred across-borders, retained or disposed within the organization
e) PII passed or shared with 3rd parties where PI is collected, created, stored, used, shared, transmitted, transferred across-borders, retained or disposed

14.4 Privacy preference and security controls specification

14.4.1. Consumer privacy preference controls

For each use case the privacy preference controls to be made available to consumer users shall be specified including:

a) The means of exercising that control directly through the product's domestic interfaces
b) The means of exercising that control via remote contact with the organization's service and communication channels.
c) Responsiveness to changes in preference for each means of exercising control

14.4.2. Consumer security controls

For each use case the security controls to be made available to consumer users shall be specified including

a) The means of exercising that control directly through the product's domestic interfaces
b) The means of exercising that control via remote contact with the organization's service and communication channels.
c) Responsiveness to changes in preference for each means of exercising control

14.4.3. Organization security controls

For each use case the security controls specific to the product to be exercised by the organization shall be specified including:

a) Technical measures to be designed into the product
b) Technical measures available by means of the organizations ICT infrastructure
c) Security processes needing the participation of employees to be effected

15. Interworking with 3rd party products

15.1 Identification of 3rd party products

If interworking with 3rd party products is required to provide product performance then as a minimum the following shall be identified :

a) the types of 3rd party products with which the product will be required to interwork
b) any specific products required for interworking to be provided by the consumer
c) any specific products required for interworking to be provided directly or indirectly by the organization
technical note: an example of directly provided 3rd party products could be Cloud services purchased by the organization and an example of indirectly provided 3rd party products could be card transaction terminals in shops for banking services.

15.2. 3rd party product interworking for privacy by design

For 3rd party products as a minimum the following shall be identified:

a) the 3rd party product security capabilities and privacy control capabilities to be utilized by the design

b) any 3rd party product specific vulnerabilities to be addressed by the design

16. General requirements for the product privacy design

The general applicability of law and regulation and standards shall be specified.

16.1. Regulations and requirements

The privacy and security regulations to be met by the design including the regulation's reference shall be identified.

The associated product requirements set for the design to meet those regulations shall be specified.

16.2. Consistency of capabilities with 3rd party products

Privacy and security control capabilities of the product interworking with identified 3rd party products shall be checked for consistency of operation.

Any deficiencies shall be documented and design requirements shall be identified to address those deficiencies.

17. Product traceability requirements

17.1. Product recall and update

The means by which the product shall be made traceable for the proposes of product re-call and product software update shall be specified.

17.2. PII traceability

If product use cases involve the passing or sharing of PII with 3rd parties then the means by which that PII can be traced for any subsequent consumer privacy related requests and control actions shall be specified.

18. Product privacy by design consumer requirements

The Consumer needs and requirements to be met by the design shall be specified for:

a) The consumer privacy controls and security needs and their derivation from use cases

b) The consumer privacy controls and security requirements and their derivation from the specified privacy needs

Technical note: this short section assumes that the informative Annex providing consumer privacy needs and their associated requirements can be used as a default checklist by users of the standard to select the appropriate consumer needs and requirements.

19. Identifying known vulnerabilities and exploits

Technical note : this section is a precursor to establishing the security requirements for the product design

19.1 Technologies for product design

The technologies to be used by the product, such as cookies, RFID, WiFi, http, optical cables, cloud services, mobile operating systems etc. shall be determined.

The known vulnerabilities of those technologies shall be identified.

The known technology vulnerabilities and exploits to be addressed in the design of the product shall be identified.

19.2. Technologies used by 3rd party products

The organisation shall determine the technologies used by 3rd party products which are necessary to deliver overall product functionality such as browsers, mobile phones and their operating systems etc.

The organization shall specify the known technology vulnerabilities and exploits associated with the 3rd party products to be addressed in the design of the product.

20. Security requirements

20.1. The security requirements to be met by the product design shall be specified.

20.2. The security requirements to be met by the design of organisational processes used to manage the product shall be specified.

Technical notes: This section could be supported by informative annexes providing well known vulnerabilities and good practice requirements for various technologies.

This section could build on, for example, the ISO standard ISO/IEC 19678 BIOS protection and other technology oriented security standards.

Further such annexes could provide organisational procedural controls available in other ISO standards.

21. Product design tools and support

21.1. The tools and support facilities to be used throughout the design process shall be identified and may include :

a) sources of design rules,
b) design tools
c) design good practices
d) design evaluation tools and methodologies
e) product privacy testing facilities

The specification of tools and support facilities shall be kept up to date with latest changes and improvements.

21.2. The support aids shall be assessed for the quality and fitness for the roles they are expected to play in assisting the design process.

Technical note: this section probably needs enhancing or supporting with at least with an informative annex providing an acceptable 'fitness for purpose' framework for design tools and support.

22. Product privacy design

Product design documentation shall be such that

a) the product's privacy capabilities provided are clearly identifiable i.e. privacy preference controls and security controls

b) the PII processed and the types of PII are clearly identifiable.

c) PII type identification shall include
    i. PII input by users

ii. the purposes for which that PII is processed identifying functional purposes, domestic processing purposes and organizational processing purposes
iii. PII created by the product within the domestic environment
iv. PII created by the product provider applications (processed on that provider's infrastructure)
v. PII passed or shared with 3rd parties
vi. other PII from 3rd parties processed by the product

d) where in the product and or 3rd party products that PII processing is undertaken

e) where anonymised data contains linkable data types

23. Product testing and validation

23.1. Testing strategy

A product testing and validation strategy and plan shall be produced that may include hardware privacy performance tests, software privacy performance tests, systems privacy tests, beta testing with real users and product privacy impact assessment.

23.2. Product hardware privacy testing

Product hardware privacy testing shall include:

a) Assessment or measurement of radio frequency eavesdropping potential of data processing resulting from radio radiation from within the consumer's hardware component of the product.

b) Assessment or measurement of radio frequency eavesdropping potential of data processing resulting from radio communication by the consumer's hardware component.

c) Assessment of physical access to the hardware that can be used to circumvent security. Hardware elements may consist of the consumer's product hardware, organisational terminals that interact with consumer's product and organisational hardware platforms.

Privacy testing procedures, methods and test equipment shall be documented.

23.3.. Software privacy testing

Product software privacy testing shall include:

a) Static code tests and checks
b) Dynamic code operation tests
c) Fuzz testing

d) Cheat testing for privacy breaking performance (such as over collection of PII and misuse of cookies) under realistic use conditions

Privacy testing procedures, methods and test software and equipment shall be documented.

Technical note: this section needs more content for good practice software testing

23.4. Product / System testing before design release from development for production

If products consist of both hardware and software and if these have been privacy tested separately then full product hardware and software integrated privacy testing shall be undertaken, including

a) Security controls
b) Privacy preference controls
c) Selected exploits

24. Privacy Impact Assessment (PIA) evaluation of the design

24.1. PIA process steps

24.1.1. The product definition shall be reviewed for the suitability to be input to the PIA process and updates agreed to that definition shall be made if the design has been changed or implemented in such a way as to impact the product definition.

24.1.2. The product use cases, design information, 3rd party product information and any other test and product design evaluation information available at the time of the PIA shall be reviewed for their suitability for input to the PIA process and updates agreed to those if the design has been changed or implemented in such a way as to impact the use cases.

24.1.3. A privacy asset value shall be identified and assigned to assets as follows:

a) the personal privacy assets of an individual

b) the organisation's assets that might be implicated with a privacy breach or loss of data

24.1.4. The threats to the privacy assets shall be identified and assessed.

24.1.5. Any additional use cases needed to address the significant risks and exploits identified in 26.1.4. shall identified and provided.

24.1.5. The vulnerabilities associated with the threats and assets shall be identified.

24.1.6. A risk assessment of the assets shall be carried out where risk is a function of asset, threat and vulnerability, taking account that there can be a number of risks.

24.1.7. Existing and new countermeasures that can be applied to mitigate risks shall be identified.

24.1.8. The residual risk shall be determined. If the residual risk is assessed to be too high then the key risk factors shall be documented and input to a review of the product development requirements.

24.1.9. If the residual risk has been reduced to acceptable levels as defined by product governance then the PIA report may be completed and signed off.

24.1.10. The PIA summary report shall be completed and endorsed to be made available in the public domain.

24.2. PIA methodology

24.2.1 PIA Overview – Privacy in Depth

The PIA for assessment of consumer goods and services designs is based on the privacy in depth model as described below.

Consumer centred

The consumer and the equipment used by consumers when interacting with the product are at the centre of the assessment. The effectiveness of the product's design is considered in the context of consumer use and threats that may arise not just from the product's digital communication with the organisation's processing but also from many other processing sources outside the control of the organisation.

Technical note: this is especially true when an organisation's online service is accessed via browsers, mobile phone and tablet apps.

Data Protection risk reduction

Many Data Protection privacy risks are addressed through the design of the product itself meeting the requirements of the relevant Data Protection authorities.

For those risks such as initial explicit informed consent to data collection the PIA process may use the Product test programmes results to ensure that the features, functions and facilities of the product deliver suitable consumer controls over their data to meet Data Protection requirements.

The privacy risk assessment focuses on the risks associated with the product in the domestic environment supplemented by assessment of risks associated with the digital communications access to an organisation's processing and the organisation's application software used to fulfil the functionality of the product.

Technical note: data loss or theft and unauthorised access to organisational data are the main risks outside the Data Protection requirements.

Human Centred

In addition to technological vulnerabilities the human vulnerabilities of consumers, the organisation's operational staff, supply chain staff and retail staff need to be taken into account.

3rd Party products

The risks associated with 3rd party products interworking needed to fulfil the products functionality, especially those 3rd party products that need to be provided by the consumer, are another key aspect of the assessment wherever those 3rd party products are not under the direct management, or contractual or process control of the organisation.

24.2.2. Determining the value of privacy risk

Technical note: For consumer choice and protection important product parameters are measured in terms that are numerically scale-able and communicable to consumers. Examples being CO^2 production by cars, energy efficiency of domestic appliances, noise production by appliances and devices. This methodology has been adopted as one that provides numerical assessment results that may be communicated to the public that is measured and reasonably understandable by unskilled individuals. This is important in notification practices related to privacy and also assists with the accurate setting of key privacy criteria by product governance.

In order to provide a measurable result from a PIA that shall be used in communicating risk levels to consumers the assessment of privacy risk values is linked to Table 1 below used to determine the risk value to PII.

Table 1 Risk value determination matrix

	Likelihood of Threat	Low			Medium			High		
	Ease of Exploitation - Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Privacy asset values shall be assigned values on a scale of 0 and 4, threat values shall be low medium or high and the degree of vulnerability to a threat shall also be assessed as low medium or high.

The matrix of table 1 using the three values shall then be used to determine the risk value.

For the purposes of assigning an asset value for use in table 1 privacy assets shall be identified with the PII associated with each asset. Each PII data type shall be assessed for privacy sensitivity and assigned a value accordingly, and then the highest value of PII data type associated with the asset shall be assigned as the asset value in the PIA.

For the purposes of determining the PIA analysis depth and scope to be undertaken within the product's budget and objectives the number and importance of vulnerabilities and threats to be evaluated shall be determined. The specific vulnerabilities and threats selected shall be listed with the criteria used for their selection.

Vulnerability, exploitability or likelihood of exploitation that is medium or high shall be included, as well as any assessment of privacy assets of value of 3 or 4.

24.2.3. Identifying privacy assets and their data

Technical note: This step in the PIA process also addresses the identification of link-ability risks inherent in product PII data sets in order to support decisions on full PIA evaluation of designs when lower inherent privacy asset values are present while they may none the less present significant privacy risks through link-ability of the product's data.

24.2.3.1. Privacy assets

In order to identify which of the possible personal privacy assets need further consideration, the potential privacy assets derived from the use case definition and specification shall be assessed to provide a set of relevant personal and organisational privacy assets that require their risks to be managed.

Such assets may include

a) personal privacy assets – tangible

i. home devices and appliances
ii. vehicles and items carried in them
iii. wearables and portables
iv. the individual's bank account (through direct access to remove funds or through payment into scams)
v. assets used for work and then taken home as part of working conditions
vi. items that are part of a larger consumer product (e.g. car parts)

b) personal privacy assets - intangible

vii. the individual's physical, physiological, mental, economic, cultural or social identity
viii. personal reputation and embarrassment,
ix. emotional balance (for example that may be at risk from those encouraging eating disorders or suicide, or cyber bullying)
x. state of health
xi. access to online ordering and financial services
xii. remote control over a domestic device

b) Organisational assets

i. Organisational tangible and intangible assets internal to the organisation that might be implicated with the loss of privacy or personal data or security breach exploit achieved via domestic equipment.

ii. Assets of 3rd party organisations that might be compromised by a product's privacy breach.

24.2.2.2. Privacy data associated with privacy assets

The PII associated with each privacy asset shall be identified together with the whereabouts of the processing of that data in the product's configuration.

The identified PII shall be used in the PIA.

The identified PII may be classified by data type in order to make the subsequent analysis and decision taking on privacy design clearer. To be added Annex 3 (ref EN 16571).

24.2.3. Requirement for a full PIA

If those data types that are designated as Personal Identifiers (PI) and Personal Behavioural Information (PB), are present in the product's consumer hardware or software or used in the organization's application software then a full PIA shall be undertaken.

Assessment of inherent identifiability of PII for full PIA

If PII of the types Personal Identifiers and Behavioural Information are not present in the product's consumer hardware or software or used in the organization's application software then the other data types shall be assessed for their inherent identifiability as data types and the personal identifiability inherent in all the product's data types in combination.

All data types shall be assessed for known link-ability to other data sets that can enhance identifiability of individuals. If known link-ability can lead to greater levels of identifiability then the inherent identifiability of the linked data sets shall be assessed.

If inherent identifiability in either the product's data set or data sets extended by high link-ability exceeds the acceptable criteria set for the privacy governance of the product then a full PIA shall be undertaken.

Note what a lesser PIA looks like has not been included in this draft. Reduced assessment may be applicable when the privacy by design process is used for low volume agile response design regimes of SME's or innovation projects.

24.2.4. Assigning PII assessment values to privacy assets

The assessment value to be assigned to an asset shall be based on the PII data types held or processed by the product on or about that privacy asset.

The criteria used as a basis for assigning a value to each PII data types shall be specified.

All PII data types associated with the specific privacy assets being valued shall be identified.

A value between 0 and 4 shall be assigned to each data types for each privacy asset to be assessed. See Annex 3 for examples

The value to be used in the PIA assigned to each asset shall be the highest PII data type value associated with the asset or by being processed on or about that asset.

Organizational privacy assets – additional considerations

The assignment of a value 0 to 4 to organizational assets may be determined using two criteria:

- the business consequences of loss or compromise of the asset, such as the potential adverse business and/or legal or regulatory consequences from the disclosure, modification, non-availability and/or destruction of information, and other personal privacy assets

- the replacement value of the asset: the cost of recovery clean-up and replacing the information (if at all possible).

Technical note :This valuation can be determined from a business impact analysis. The value, determined by the consequence for business, is usually significantly higher than the simple replacement cost, depending on the importance of the asset to the organization in meeting its business objectives. Consequences or business impact may be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or past data.

24.2.5. Ease of exploitation of vulnerabilities

For the purposes of assigning a value to the likelihood of threats to the product's known product design, vulnerabilities shall be identified for the design being assessed by the PIA.

Note: Examples of vulnerabilities could be for example use of unencrypted radio links, use of a mobile phone operating system with known privacy breaking exploits that allow privacy settings to be changed without the (consumer) PII Principle's knowledge.

The design's ability to overcome these known vulnerabilities shall be assessed and a value shall be assigned to the likelihood of a threat to PII stored or otherwise processed by the product.

Technical notes: the vulnerabilities may be considered with respect to :-

Confidentiality refers to limiting information access and disclosure only to authorized users
Integrity refers to the trustworthiness of the information source.
Availability refers simply to the availability of the information resource

In addition to the existence of exploitable vulnerabilities in the design, the likelihood of a threat may be related to the assessed cost of exploiting the design vulnerability where a low cost equates to higher likelihood and higher cost relates to lower likelihood.

Further to the existence of exploitable vulnerabilities in the design, the likelihood of a threat may be related to the exposure time that a product may be subject to any threats including for example allowance for known hacking behaviours that delay exploitation until product volumes are higher or product support removed.

The criteria used as a basis for assigning a value to each threat likelihood shall be specified.

The values assigned to each threat shall be one of three values low, medium or high.

24.2.6. Assigning likelihood of exploitation of vulnerabilities

For the purposes of assigning a value to the likelihood of vulnerability exploitation to avoid both unjustified public concern or organisation denial, the likelihood value shall be based on reputable independent evidence.

Technical notes: For product designs that have been released to the public the intent is for independence to be without direct or indirect sponsoring from those with an interest in concealing vulnerability exploitation but is not meant to imply that the evidence of vulnerabilities exploitation has to be in the public domain as organisations may have good reasons for not publishing vulnerabilities or their exploitation to reduce the knowledge in malicious communities

For product designs during the product development stages when details of the design may not be accessible to independent 3rd parties independence in exploitability assessment may be addressed by independent experts within the product organisation or contracted 3rd party experts making an assessment under commercial confidentiality.

The process is intended to ensure that justified independent evidence is not ignored by those using the standard.

The likelihood rating used for table 1 shall be:

a) Zero likelihood = technically impossible
b) Low likelihood = theoretical validation of exploitability from a reputable source
c) Medium likelihood = proof of concept validation of exploitability from a reputable source
d) High likelihood = vulnerability being exploited in the market place evidenced by reports from consumers and professional sources.

Adjustments to the technical assessment may be made subject to risk exposure by numbers of individuals potentially affected and the exposure time of those individuals to the hazards. The criteria used for any such adjustments shall be documented and be subject to approval by the product's privacy governance.

24.2.7 Identification of mitigation mechanisms

24.2.7.1. Where risk assessment ratings in the range 0 and 8 exceed the criteria set for the PIA risk assessment mitigation measures shall be identified. The risks shall be reassessed with the mitigation measures applied using the PIA methodology.

24.2.7.2. Where re-assessment of the risk after allowance for the mitigation measures identified still exceeds the criteria set for the PIA then the product design requirements impacting consumer privacy shall be reviewed to address the outstanding PIA assessment issues with the design and mitigation measures.

If this occurs then the PIA issues with the design and mitigation measures shall be documented.

24.2.8. Where the PIA evaluation criteria for the design have been met and when all other product release criteria have also been met then the design may be released for production.

Note: PIA report and summary requirements to be developed in later drafts

25. Production privacy protection of the design

25.1. Preparation for production

25.1.1 Specifications
The production facility shall have the product's specifications including the design to be released to the market, performance criteria, components and subassemblies, assembly requirements, final production testing, packaging and labelling.

25.1.2. Components and subassemblies
Before production begins checks shall be made that components and subassemblies to be used in production meet the design specifications and are neither at their end-of-life nor unapproved replacements.

25.1.3. Goods in checks
In order to mitigate the risks of 'infection' of components used in the main design, every batch or delivery of components or subassemblies shall be checked for compliance with their design specifications including checks for privacy affecting hidden features.

Inventory management shall ensure that components and subassemblies can be traced to their source, batch, lots and date.

25.1.4. Other pre-production checks
In order to ensure that the product can be produced consistently in compliance with specifications at the required production rate the following shall be undertaken:-

a) confirming that the final design is the one to be used for actual production
b) review of any prototypes built prior to production

In addition, completing a pre-production run may be undertaken.

25.2. Production defects

Production defects shall be monitored and corrected.

Production processes shall monitor hardware production for defects that impact privacy.

Technical note: for example, production defects that reduce sensor accuracy of PII or touch sensitivity for privacy controls, loose fixings that allow easy access to inner circuitry for malicious purposes etc.

Software production shall monitor sources of software components from 3rd parties for clean versions of the software components incorporated into the design.

Software design versions shall be checked to ensure that the correct versions are used for product production.

Software distribution servers shall be monitored for malware affecting production software to be distributed to others.

26. Production testing and system commissioning

Design implementation post production in products shall be validated for the expected privacy protection capabilities of the design.

Technical note: It is possible for product build to not match that of the prototypes tested or expected design and so validation of the design as implemented for the consumer is needed.

27. Incident monitoring and response planning

27.1. An open reporting mechanism for privacy / security incidents, investigations, complaints and concerns from professional bodies and the public shall be put in place.

Inputs from professional bodies and the public shall be acknowledged.

Confidentiality with respect to individuals providing feedback shall be protected.

27.2. If the design incorporates one or more of the elements hardware, software or firmware the mechanisms for the following shall be put in place :

Software: a) and b)
Firmware: c)
Hardware: d) and e)

a) Software updating
b) If software updating is to be provided online mechanisms for ensuring the mutual authentication of software source and destination of the update.
c) Firmware updating
d) Hardware recall
e) Hardware withdrawal

27.3. The mechanisms a) to e) shall be validated as fit for purpose before product release.

Technical note:
ISO/IEC 29147 Vulnerability Disclosure, ISO/IEC 30111 Vulnerability handling and ISO/IEC 27043 Technical vulnerability and exploits reporting should form the basis for additional good practice requirements in this section.

27.4. Product registration to facilitate design risk mitigation action

A product consumer registration process shall be provided that is easy to understand and use by non-expert consumers. Registration processes may include:

- online forms
- paper forms
- automated online mechanisms realized through the product design

If an automated product registration processes is used then explicit consumer consent to that registration shall be obtained.

28. Pre-Product release retail channels privacy review.

Technical note: There are privacy implications to how retail channels are involved in bringing products to consumers as originally highlighted in the European RFID PIA standard EN 16571 as well as good practice such as that identified by OFCOM in the UK for retail sources of apps. This section is incorporated to ensure such risks are adequately addressed prior to product launch. Retail channel consumer use cases may be required depending on the nature of the product and its channels.

In order to determine and address any significant privacy risks arising from the means by which consumers access or purchase the product: -

28.1. A review shall be undertaken of the retail and or access channels to be used for the product including:

a) Any privacy risks associated with the chosen retail channels and the steps proposed to mitigate those risks.
b) Consumer facing staff product privacy information to be associated with product sales, marketing and support.
c) Any product contact terms that impose unfair privacy risk consequences on consumers and correction thereof

28.2. Any retail and or access channel residual privacy risks shall be documented and communicated to the retail channels.

28.3. Any retail channel staff and consumer product privacy information deficiencies shall be corrected before product release.

29. Documentation – consumer, regulatory, sales and support

29.1. A review shall be undertaken of the following consumer documentation elements.

a) Privacy labelling of the product
b) Supplementary privacy information and its method of provision to consumers
c) Consumer consent mechanisms and their information content necessary to meet Data Protection requirements
d) PIA summary information
e) Radio emissions distances for operation and eavesdropping performance
f) Signage associated with product use and privacy protection in public spaces
g) Product consumer security and privacy control operational instructions
h) Consumer reporting of complains and incidents forms to be used by consumers completeness and clarity

29.2. Any consumer documentation, labelling and signage deficiencies shall be documented for the purposes of correction pre-product release.

29.3. Any consumer documentation, labelling and signage deficiencies shall be corrected before product release.

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

29.4 Regulatory information

29.4.1. A review shall be undertaken of the availability of documentation required for provision to regulators.

29.4.2. Any regulatory documentation deficiencies shall be documented for the purposes of correction pre-product release.

29.4.3. Any regulatory documentation deficiencies shall be corrected before product release.

29.5. Product sales, marketing and support channel information

29.5.1. A review shall be undertaken of the availability of documentation required for marketing, sales and support of the product.

29.5.2. Any sales, marketing or support documentation deficiencies shall be documented for the purposes of correction pre-product release.

29.5.3. Any sales, marketing or support documentation deficiencies shall be corrected before product release.

30. Product release to market

30.1. Design privacy review

A product privacy fitness for release report shall be produced detailing product privacy checks, regulatory and testing conformances, the PIA assessment rating for the release design level and residual risks and mitigations.

30.2. Readiness of retail channels

The preparation of retail channels with privacy information, any required sales staff training and sales processes shall be checked and deficiencies identified and documented.

Any deficiencies in the privacy readiness of retail channels shall be corrected before product release.

Confirmation of readiness shall be provided when all specified retail channel attributes have been achieved.

30.3. Readiness of product support

The preparation of product support with privacy information, any required product support staff training and product support processes shall be checked and deficiencies identified and documented.

Any deficiencies in the privacy readiness of product support shall be corrected before product release.

Confirmation of readiness shall be provided when all specified product support attributes have been achieved.

30.4. The senior business manager responsible for privacy governance shall determine whether the product at that design level may be released to market as far as it's privacy design, market monitoring, privacy preparation of sales and support and preparation for post release product corrective action is concerned.

31. Market monitoring

31.1. The means by which feedback from consumers and other users is obtained shall be monitored and reviewed to determine whether significant privacy risks, as determined by product privacy governance, occur in the market.

31.2. The market shall be monitored for

a) unanticipated use of the product
b) exploitation of product vulnerabilities
c) exploitation of vulnerabilities in 3rd party product affecting the product
d) professional reports on product vulnerabilities and exploits

e) changes in regulatory requirements
f) any other factors identified by product privacy governance

31.3. Consumer privacy affecting incident reporting and consumer concerns reporting

Consumer feedback shall be provided using understandable feedback forms supported by customer information databases.

Consumer feedback may be supplemented by automated data collection from the product with associated consent to the collection of that data.

31.4. Monitoring mechanisms may include:

- Well organized customer service response and claims department (e.g. call centers)
- Monitoring of social network for customer feedback and prompt action
- Systematic recording and evaluation of incidents, claims, and complaints
- Reports and feedback from retail, access and distribution channels
- Security reports from 3rd party security experts
- Reports from 3rd party interworking product providers
- Full and comprehensive privacy risk analysis and trend analysis and implementation of corrective actions
- Use of customer focus groups for product use and product privacy evaluation
- Review of changes in market conditions and regulatory requirements
- Feedback from operational staff
- Checks that all service work conforms to the expressed service provided (no deviations or additional services, service conforms to design specifications, no non-approved modifications)

31.5. Validation of vulnerability and exploits

The reported vulnerabilities and exploits shall be tested and/or assessed for the validity of the reports.

31.6. Identifying the need for corrective action

31.6.1. Corrective action shall be initiated when the criteria set by product governance for product privacy performance are no longer met.

31.6.2. Action on the product's privacy design may be initiated for other reasons.

Technical note: product design and privacy capabilities may need to be upgraded for example for competitive reasons, or to meet the privacy needs of new market segments to be addressed under business development objectives.

31.7. Prioritising privacy risk corrective action

31.7.1. An iteration of the product's privacy impact assessment shall be undertaken to assist problem prioritisation. Prioritisation assessment shall include as a minimum

- the sensitivity of the information revealed from the privacy breaking exploit
- direct revealing of PII

- linkable data that combined with other data sets has enabled significant levels of privacy impact
- numbers of people directly affected or at risk
- the severity of harm caused to individuals by the exploit. Harm assessment to include: physical safety, financial, reputational, and emotional harm
- impacts on the organisation – increased security risks, financial, reputational etc.

31.7.2. Corrective actions

Action shall be prioritised to categories to which product governance may assign resources to address the issues or may add to ongoing product development requirements.

31.8. Identification of sources of privacy risk to be addressed

31.8.1. Unanticipated use

If unanticipated use has created the prioritised privacy risk then additional use cases shall be created or current use cases shall be updated.

The design shall be reviewed and updated using the new and or updated use cases and the design process shall iterate to create an updated design and product documentation for current users.

31.8.2. Product vulnerability exploits

If new or known product vulnerabilities have created then the product security requirements shall be reviewed and updated.

The design process shall iterate with the updated security requirements to create an updated design and product documentation for current users.

31.8.3. Third party vulnerability exploits

If product privacy exploits involve the exploitation of vulnerabilities in 3rd party products then:

a) product security requirements shall be reviewed and updated
b) exploits reports shall be provided to the providers of the 3rd party products

The design process shall iterate with the updated security requirements to create an updated design and product documentation for current users

32. Privacy breaches - remedial action.

32.1. The proposed remedial action to be taken for a prioritised privacy exploit shall be determined and approved by the senior business manager responsible for the product privacy governance.

32.2. Privacy exploit and remedial action information for regulators shall be prepared and made available to those regulators where the product is sold or accessed and where regulations require such notification.

32.3. Consumer mitigation action

If consumer mitigation action is required then

32.3.1. The consumers immediately affected shall be identified

31.3.2. Consumers who may reasonably be considered to also be at risk shall be identified

32.3.3. Consumer information shall be prepared to clearly and understandably communicate to non-expert users:

a) the exploits and risks requiring consumer mitigation action
b) the actions to be taken by consumers to mitigate those risks
c) consumer feedback mechanisms if those mitigation actions present unanticipated difficulties for consumers

Consumer product mitigation action information shall be distributed to consumers.

Consumer communication channels for risk mitigation shall be determined and used. Such channels may include:

- e mails to registered users
- web site notifications
- TV and radio adverts
- social media
- letters to consumers
- product information ‘pop up’ screens if the product is online and has a user screen communication capability

32.4. Product software and or firmware code update mitigation action

If the product’s software or firmware is to be updated then the update code to be uploaded to consumers’ products shall be checked and validated for release.

If the product’s software or firmware is to be updated then the distribution sources of the update code shall be checked and validated for clean code distribution.

If automated updating of software and firmware has been designed into the product then that shall be initiated subject to explicit consent from consumers for such updating action.

If product software and firmware update is not automated then availability of the update shall be distributed to consumers

32.5. Product recall mitigation action

If product recall is required to allow product provider direct intervention in updating the product to mitigate risks then consumer information shall be prepared to clearly and understandably communicate to non-expert users:

a) the exploits and risks requiring recall mitigation action
b) the actions to be taken by consumers to effect recall
c) consumer feedback mechanisms if those recall actions present unanticipated difficulties for consumers

Consumer product recall action information shall be distributed to consumers.

Consumer communication channels for recall mitigation shall be determined and used. Such channels may include:

- e mails to registered users
- web site notifications
- TV and radio adverts
- social media
- letters to consumers
- product information 'pop up' screens if the product is online and has a user screen communication capability

32.6. Other mitigation actions

If mitigation action is required by organisations other than the product organisation then that action shall be specified and the associated communication to inform the other parties put in place.

Non product organisations may include:

- retailers
- support agents
- 3rd party product providers
- police and security agencies
- regulators

32.7. Monitoring effectiveness of product mitigation actions

A product mitigation action monitoring process shall be established.

Product mitigation effectiveness shall be reported to the senior business manager responsible for product privacy governance.

If mitigation action is of low effectiveness as determined by the product's privacy governance then the senior business manager shall consult with stakeholders to determine additional action. Such additional action may include:

- further consumer communication
- adding consumer incentives to take action
- product withdrawal from sale or new access
- use of 3rd parties to support mitigation actions

33. Maintaining privacy protection at end of product life cycle

Technical notes: Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be changed market demands, further technology innovation, or the products maturing and needing to be functionally richer technology.

Determining the issues faced by consumers can be addressed through stakeholder engagement and developing end of life use cases allowing for technical and behavioural issues to be analysed and addressed.

The good practice drafted in the following sections addresses issues when market and lifecycle conditions determine that a product's end of life has been reached and

then subsequently a significant number of users stay with the withdrawn product for a prolonged period of time.

33.1 Determining whether withdrawal conditions have been encountered

If the product has reached point in the market where it's withdrawal from sale and or support has been reached as determined by the end of life criteria established by product governance then a product end of life policy shall be determined.

End of life criteria may include:

- severity of re-design requirements costs and timescales
- product profitability and/or operating costs
- product technology lifecycle (for obsolescence)
- availability and support for 3rd party products needed for the product to fulfil its functions

The product end of life withdrawal policy shall include policies addressing consumer privacy issues. The product end of life withdrawal privacy considerations may include:

- Numbers of consumer users
- Dependency of consumers use of the product to sustain their safety and health
- Availability of suitable alternatives at reasonable cost
- Determining the withdrawal phase support to the product to be provided if consumers, who are dependent on the product, would be made significantly more vulnerable without it until suitable alternatives can be found.

Product end of life policies may also include:

- End-of-Sale Notice Period
- Operating System Software maintenance support
- Add or attach new service contracts
- Renew service contracts – for HW & Operating System SW
- Hardware Repair or Replacement
- Customer Service and Support of HW & Operating System SW
- Application Software maintenance support
- Renew service contracts – for Application SW
- Customer Service and Support of Application SW
- Addressing residual privacy queries and support issues
- Major incident response if significant numbers of consumers are affected

The effectiveness of the end of life withdrawal process shall be monitored to maintain interim privacy support while significant numbers of consumers depend on the product

33.2. Consumer communication

If product end of life withdrawal is required then consumer information shall be prepared to clearly and understandably communicate this to non-expert users.

Product end of life withdrawal consumer information shall include:

a) consumer options if they are to continue using the product
b) consumer alternative products
b) privacy protecting actions to be taken by consumers resulting from product end of life withdrawal
c) consumer feedback mechanisms if product sale or additional access withdrawal presents unanticipated difficulties for consumers

33.3. Consumer product withdrawal information shall be distributed to consumers.

Consumer communication channels for withdrawal shall be determined and used. Such channels may include:

- e mails to registered users
- web site notifications
- TV and radio adverts
- social media
- letters to consumers
- product information ‘pop up’ screens if the product is online and has a user screen communication capability

33.4. Retail channels actions

Product retail channels shall be briefed on action needed to provide privacy protection on obsolete or near to obsolete products in stock.

32.5. Product withdrawal product privacy support

If sufficient consumers continue to own or use product withdrawn form sale then interim product privacy support shall be put in place. Interim support may be provided within organisation and or via 3rd parties.

Maintenance of interim withdrawn product privacy support shall be determined by product privacy governance.

32.5.1. Interim withdrawn product privacy support

Interim withdrawn product privacy support shall be provided with up to date product information, training and support processes.

The conditions for sustaining interim support shall be monitored.

The quality of interim support shall be monitored

Feedback of market exploits and non-design change mitigation actions shall be maintained until privacy support is also withdrawn.

- end -

Annex 1 - Informative list of Consumer Privacy Needs

Note: the associated consumer product requirements should be added in later drafts.

1 General consumer domestic privacy needs

1.1 Security of domestically used digital equipment (hardware and software)

1.1.1 Network and system security

1.1.2 Consumer digital devices security

1.1.3 Keeping consumer protection up to date

1.1.4 Sourcing trustworthy apps and applications

1.1.5 Loss of digital devices

1.1.6 Consumer device security over a product lifecycle

1.1.7 Consumer security information

1.1.8 Consumer confidence in organisations' terminal equipment

1.2 Consumer domestic personal processing privacy control

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

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

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

1.2.4 Consumer privacy control for remote control of Things

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

1.3 Consumer control over their data sharing over social media

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

1.3.2 Privacy controls with respect to those receiving shared personal information

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

1.4 Privacy and intrusive content

1.4.1 Consumer privacy controls for intrusive content

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

1.5 Consumer privacy control over data collection by third parties

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

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

1.5.3 Consumer privacy and service interactions

1.6 Privacy in public places (physical and virtual spaces)

1.6.1 Personal data analysis that removes anonymity

1.6.2 Anonymity when personal information is collected via sensors

1.7 Personal accountability for online views

1.7.1 Accountability for statements and views made online:

1.7.1.1. Direct to individuals

1.7.1.2. About individuals in public virtual domains

2 Consumer privacy needs when personal data is transferred and traded once it has been collected

2.1 Personal data traceability and transparency to support data protection law
2.1.1 General personal data transfer traceability
2.1.2 Traceability of transferred data for consumer consent

2.1.2.1 Consent to new processing purposes

2.1.2.2. Consent traceability within original data processing consents given
2.1.3 Traceability of transferred data for the purposes of personal data access and correction requests

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

2.2 Managing personal data transfer traceability requests

2.2.1 Valid traceability of data sharing requests

3 Using Consumer Personal Data (data analysis)

3.1 Balancing the right to privacy with the public interest

3.1.1 Governance
3.1.2 Engaging stakeholders

3.2 Anonymization
3.3 Re-identification
3.4 Profiling: Building up large personal profiles
3.5 Data fitness for purpose

3.6 Existing customer or client data analytics

3.7 Analysis of PII from open data

3.8 Data analytics to identify or target an individual

3.9 Data analytics to identify groups of people
3.10. Data analytics for systems

4 Strategic Consumer Privacy Needs

4.1 The Right to be Forgotten
4.2 Privacy by Default
4.3 Privacy by Design

5 Additional needs of developing economies

Currently under development within COPOLCO

6 Protection needs - Privacy Impact Analysis for consumer digitally connected devices (The key risk areas that consumer digital device PIA's need to address)
6.1. Remote control over device power
6.2 Eavesdropping digital radio emissions from devices
6.3 Data transmission to and from the connected device (security)
6.4 User control of data types passed over networks and remote processing of that data
6.5 User personal data sensitivity
6.6 User control over personal privacy preferences

6.7 User behaviours
6.8 User privacy exposure arising from organisational security breaches

7. Privacy information to be provided to consumers

7.1 Public place privacy awareness notification and signage

7.2 Consumer product/service information

7.2.1 Summary of privacy impact assessment

7.2.2 Privacy risks and mitigation actions
7.2.3 Privacy control instructions
7.2.4 Privacy and security of domestic equipment maintenance instructions

7.3 Consumer Privacy Information Policies

7.4 Privacy risks and mitigation actions

7.5 Privacy labelling

7.6 Privacy complaints and queries

8 Privacy protection when an organisation loses personal data

8.1 Within organisation action to prevent/reduce subsequent fraud resulting from the data loss

8.1.1. PII (personal information) loss by the organisation

8.1.2 PII loss by another organisation that could be used for fraud etc.

8.2 Information for consumers about precautionary action and advice in the light of the data loss

8.3 Consumer action to be taken if the consumer detects fraud arising from data loss

Annex 2 Informative Annex – *to be developed*

Guidance on privacy design using common technologies

Examples of common technologies

- Internet protocols
- Internet and web formats
- Data schemas
- Web APIs
- Device APIs
- RFID tags and readers
- Web service definitions
- Browser plug-ins
- Proximity and connectivity standards for promoting data sharing, device coupling and service invocation
- Collaborative applications/services
- User experience and UI control
- Mobile applications and services

Annex 3 – Examples of Personal Privacy Assets and associated PPI numerical rating for sensitivity

Technical note: A fuller set can be seen in the RFID PIA standard CEN EN 16571 Annex H

Examples of privacy assets

- Passport
- Driver licence
- Medical monitoring device
- Mobile phone
- Retail loyalty card
- Medical sample
- Smart / tagged clothing
- Digital music downloads
- Smart domestic appliances
- Remote controlled garage doors
- Vehicles
- Toys
- Library books
- Sports or event ticket

Examples of PII sensitive rating for asset value assignment

Data type	value to be assigned	(comments)
Name	2	
Unique personal code	3	
Telephone number	3	
e mail address	3 - 4	(3 if anonymous 4 if an identifying name)
Date of birth	2	
DNA	4	
Digitized biometric finger	4	
Digitized biometric face	3-4	
Address	2	
Nationality	2-3	(possibly more sensitive if not a national)
Racial origin	2-3	
Account details	3	
Court offences	3	
Health status	3	
Religious belief	2-3	(majority belief in the culture 2 minority belief 3)
RFID chip ID	2	
Mobile phone ID	2-3	(depends on exactly which id)
MAC addresses	2-3	
Residual values on various smart cards	1-4	(depends on average residual value)
Location	2-3	(depends on accuracy of location data)
Retail product code	0-3	(depends on objects conveying beliefs or behaviours or financial values