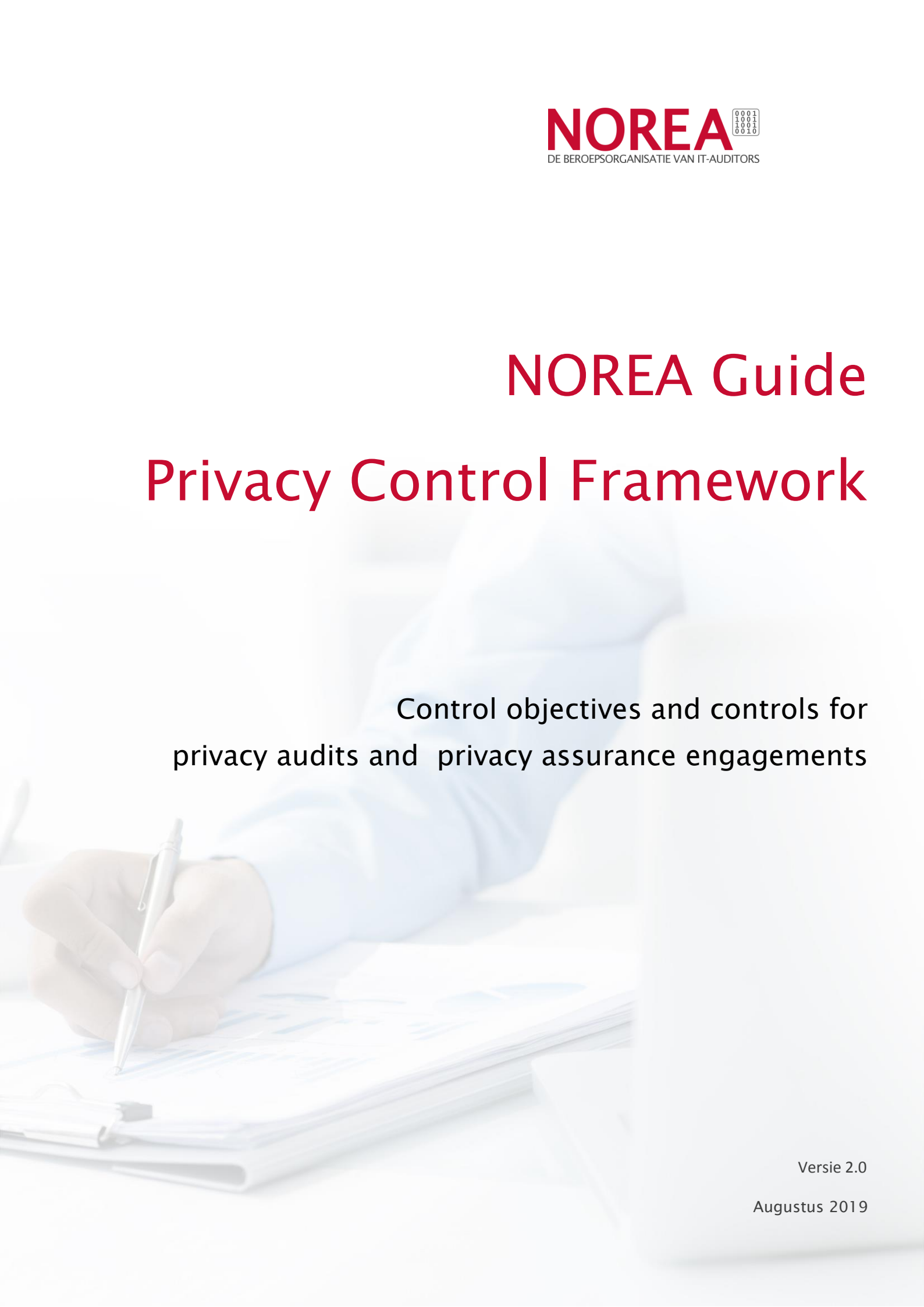
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA Guide

Privacy Control Framework

Control objectives and controls for
privacy audits and privacy assurance engagements



Versie 2.0

Augustus 2019

Acknowledgement

This guide (in Dutch "Handreiking") is issued by NOREA, the professional association of IT-auditors in the Netherlands and was developed to guide Dutch chartered IT-auditors (Register IT auditors, RE's) in issuing assurance reports in alignment with the European General Data Protection Regulation (GDPR) and the relevant standards on assurance engagements.

Working group participants

On behalf of the NOREA Expert Committee Privacy and the Working Group Privacy Control Framework the following persons contributed to the development of this framework:

drs. Jaap Boukens RE RA, Jeroen Caron RE MSc CIPP/E, ir. Jan de Heer RE, Maurice Koetsier MSc RE CIPP/E CIPM, Henk van der Linde RA, mr. Winfried Nanninga RE CIA MMC, ir. Ali Ougajou RE, drs. Ed Ridderbeekx RE CISA CIPP/E, ir. Elisabeth Lekkerkerker-Smit RE, Maurice Steffin RC CIPP/E CIPM

Coordination and editing

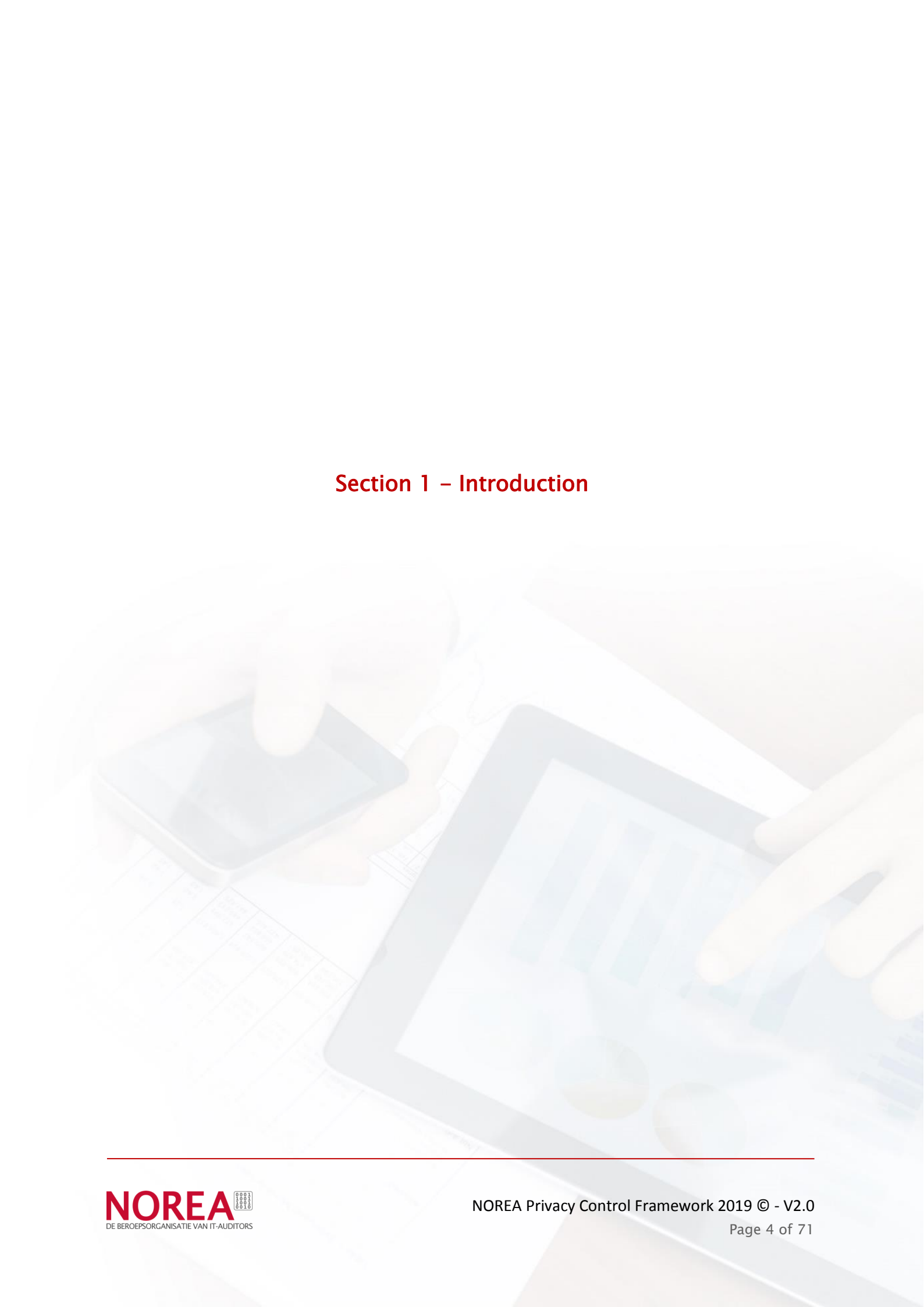
Version 1.0: ir. Jan de Heer RE, drs. Ed Ridderbeekx RE CISA CIPP/E
Version 2.0: drs. Ed Ridderbeekx RE CISA CIPP/E

PO box 7984, 1008 AD Amsterdam
phone: +3120-3010380
e-mail: norea@norea.nl
www.norea.nl

Version control		
Version	Date	Amendments
1.0	May 2018	
2.0	August 2019	Refer to subsection 10 in Introduction

Table of contents

Section 1 – Introduction



1. Introduction

This document presents the Privacy Control Framework developed by NOREA (Dutch Association of chartered IT-auditors / Nederlandse Orde van Register EDP-auditors), henceforth referred to in this document as "PCF".

2. Objectives of the Privacy Control Framework

The PCF's primary objective is to provide guidance to (audit) professionals in assessing whether an entity's control objectives regarding privacy and personal data protection are achieved. As such, the PCF can be used as the starting point for tailored privacy audits. The PCF contains the prescribed control objectives and illustrative controls for privacy assurance assignments based on the Assurance 3000 standard ('NOREA Richtlijn 3000'). It can also be used to help constitute the privacy section of a SOC 2® assurance report in an entity that has to comply with the General Data Protection Regulation (GDPR).

In addition, the PCF can be deployed by an entity to assess the adequacy of privacy controls or to determine the extent to which current controls should be adapted to comply with (changing) legislative frameworks (e.g. the GDPR).

3. Structure of the Privacy Control Framework

The PCF is based on an information lifecycle model and the following 'best practice' frameworks:

1. GAPP Principles – issued by the AICPA/CICA;[1]
2. NIST SP800-R53 Privacy Control Catalog;[2]
3. The NOREA Raamwerk Privacy Audit;[3]
4. EuroPriSe framework.[4]

A more extensive explanation of the information lifecycle is provided in Annex 2. For each phase, applicable privacy topics have been established, which are identified by a three-letter abbreviation (32 in total). Each privacy topic is linked to a control objective to be achieved, which subsequently has been operationalised by a number of controls to be evaluated (95 in total).

[1] An Executive Overview of GAPP: Generally Accepted Privacy Principles, 2009.

[2] Security and Privacy Controls for Federal Information, Systems and Organizations, NIST SP800-R53 Privacy Control Catalog, 2013

[3] The NOREA Raamwerk Privacy Audit, 2005, Addendum Norea Privacy Audit bij Richtlijn 3600n, 2017

[4] European Privacy Seal EuroPriSe, 2008

Section 2 provides an overview of the privacy topics and their associated control objectives. Section 3 contains a detailed list of the controls per topic.

4. Privacy Control Framework and the GDPR

The control objectives and illustrative controls of the PCF are prominently aligned and cross-referenced with 13 GDPR key elements. This was done based on professional judgement and the topics addressed in the document 'In 10 stappen voorbereid op de AVG' by the Autoriteit Persoonsgegevens (Dutch Data Protection Authority). An entity using the full set of PCF criteria is obliged to address these main topics from the GDPR, and to have controls in place which ensure that applicable objectives required by law are met.

By implementing and operating PCF controls, reasonable assurance can be achieved that the associated control objectives are met. Although the PCF's control objectives and controls are aligned with GDPR principles, adhering to the PCF by definition cannot guarantee full compliance with the GDPR. The GDPR is a comprehensive law that contains many detailed requirements for specific circumstances, not all of which have been addressed in the PCF for reasons of practical usability.

Professionals assessing the privacy control environment of an entity (including, for example, a gap analysis regarding GDPR readiness) are encouraged to refer to additional material to assist them in identifying and considering specific legal requirements (e.g. the Uitvoeringswet AVG) and authoritative guidance (e.g. by the European Data Protection Board, EDPB) that are applicable to the entity under assessment.

Cross references between the PCF and the GDPR are provided in Annex 1 of this document.

5. Use of the Privacy Control Framework

The way the PCF is used in practice depends on the objectives of the user. In general, three types of users are distinguished:

a. An IT-auditor who assesses an entity's privacy controls and the achievement of privacy objectives with the objective for example to assess privacy maturity or GDPR-compliance;

b. An IT-auditor who performs a privacy assurance engagement, based on standard 3000 ('NOREA Richtlijn 3000'), or an assurance engagement based on SOC 2 in an entity where privacy is governed by the GDPR. In addition, an IT-auditor uses the PCF if the standard 3000 engagement is performed to substantiate the issue of a Privacy Audit Proof® seal;

c. Other professionals (such as risk managers, data protection-, security-, and privacy officers) who aim to assess an entity's privacy maturity or GDPR-compliance (non-audit) of an entity.

It is assumed that the scope of any of the audits or engagements mentioned above will be defined as (a) a clearly described, specific, and risk-based (set of) processing operations of personal data by the entity.

The PCF provides an indication whether a control is relevant to an entity as a controller or to an entity in the role of processor, or both. This is indicated with the letters 'C' and 'P' in a separate column next to each control in section 3. This should be related to the scope of an assessment or engagement. If an entity is a controller or a processor for at least one processing activity in scope, the controls flagged as 'C' or 'P' respectively, apply.

Privacy control assessments

For privacy control assessments, the IT-auditor involved can use the PCF as a general framework and tailor it to the scope of the assessment to be performed. A good starting point to do so is to consider the privacy topics and associated control objectives in section 2 and take a selective approach to match the engagement scope. As a second step, for the topics and objectives selected, the IT-auditor can determine which controls from section 3 should be evaluated. It is at the IT-auditor's discretion to modify or enhance the controls to optimally fit the engagement's scope and purpose.

Assurance engagements

In the case of privacy assurance engagements, the PCF can serve as the basis for criteria to be embedded in assurance reports along the 3000 standard ('NOREA Richtlijn 3000'). Use of the PCF is required if the standard 3000 assurance engagement is performed to substantiate the issue of a Privacy Audit Proof seal.). It can also be used to help constitute the privacy section of a SOC 2 assurance report in an entity that has to comply with the GDPR (see also subsection 6 below).

In performing the privacy assurance engagement, the IT-auditor may integrate all topics and control objectives in section 2 in the assurance scope and reference these as the applicable control framework in the assurance report. Regarding the controls from section 3, the IT-auditor carefully considers which controls are applicable for and will assure achievement of the control objectives of the entity. The controls in section 3 provide examples; it is the entity's responsibility to enhance or modify them where necessary, given the characteristics of the entity. The controls thus selected can be tested by an independent IT-auditor to obtain sufficient and appropriate assurance evidence for an objective opinion.

Given the fact that the GDPR requires organisations to *demonstrate* control of personal data protection, it is obvious that the PCF will be predominantly used in attestation assignments.

6. PCF and other NOREA privacy instruments

The PCF is an element of (and related to) a broader set of privacy related instruments that NOREA offers to practitioners. These are the following:

- *Guidance for Privacy Impact Assessments*
  At the time of writing of the PCF 2.0, this guidance for performing data protection impact assessments (DPIA's) is being revised to be brought entirely in alignment with the GDPR. The current version 1.2 (2015) is expected to be replaced by an updated version in the second half of 2019. Performing DPIAs (also refer to the 'PIA'-topic in this document) provides clarity in privacy risks. To mitigate these risks, the control objectives and controls from the PCF can serve as a basis.

- *Privacy principles and criteria for SOC 2*
  Work is also in progress to make an addition to NOREA's 'Guidance to Richtlijn (ISAE) 3000 Service Organization Control Reports for IT Service Organizations, based on the AICPA SOC 2 report model and the Trust Services Principles and Criteria'. This addition outlines how the privacy category can be included in an ISAE 3000 / System and Organisation Control Report based on the SOC 2 report model and the underlying Trust Services Criteria. For that purpose, a mapping was made between the SOC 2 Trust Services Criteria and the PCF control objectives.

  It is mandatory to report on the SOC 2 privacy criteria in a SOC 2 report. NOREA's guidance explains how the PCF's illustrative controls can be used as guidance to substantiate the SOC 2 privacy criteria, while taking into account the purpose (objective) of the (service) organization and the 'points of focus'. As soon as the addition is completed it will be published on NOREA's website.

- *Privacy Audit Proof seal*
  Based on an assurance assignment that resulted in a positive opinion from a privacy (IT-) auditor, permission can be granted to a controlling or processing entity to use the Privacy Audit Proof seal (logo), for which the PCF is the point of reference as the underlying normative framework. Use of the PCF's control objectives is required; the PCF's controls are illustrative. The seal can only be issued on the basis of an assurance assignment, performed along Richtlijn 3000 (Assurance assignments by IT-auditors) providing reasonable assurance and without limitations in the opinion. The regulation ('reglement') for Privacy Audit Proof is currently under revision to reflect these rules.

7. PCF and GDPR certification

The GDPR itself emphasizes the importance of certification mechanisms to demonstrate GDPR compliance. In spite of the fact that the PCF at the moment should not be regarded as a set of

criteria that formally enables a certification as referred to in articles 42 and 43 of the GDPR, in principle it complies to the guidelines the EDPB has published on GDPR certification[5].

In the Netherlands, the Autoriteit Persoonsgegevens (AP) propagates a model in which the development of certification schemes and criteria is left to the market. Audit organisations wishing to issue 'GDPR certificates' – in fact, the future Certification Institutions (CI's) – will first have to be accredited to be able to do so. The AP has put this task into the hands of the Raad voor Accreditatie (Dutch Accreditation Body, RvA). At this stage (per August 2019), no CI's in the Netherlands have been accredited yet.

While establishing the PCF, NOREA has met various times with representatives of the AP and the draft version of the PCF was submitted to the AP for comments. As a response, the AP expressed its appreciation for the (further) development of the PCF as an important standard for audit professionals.

At this stage, it is not yet possible to acquire a formal certificate as referred to in articles 42 and 43 GDPR. It is, however, possible to obtain a privacy assurance statement as a result of an audit performed by an independent IT-auditor on the basis of the PCF criteria. It is expected that in the future these schemes (certification and assurance) will move towards each other. New developments in this area will be published on NOREA's website.

In the meantime we recommend organisations, interested in obtaining a GDPR- certificate or privacy assurance statement, to contact an IT-auditor certified by NOREA.

8. PCF and ISO 27001/27002

Personal data should be regarded as a special occurrence of information, which in the context of privacy requires adequate protection. As such, there obviously is a strong relation *and* a certain amount of overlap between the PCF and normative frameworks for information security in general. Examples of the latter are NEN-ISO/IEC 27001 and 27002, which serve as a standard for certification purposes of an information security management system (ISO 27001) and as a set of guidelines and best practices in information security (ISO 27002). Many other frameworks (such as the Baseline Informatiebeveiliging Rijksdienst (BIR)) have their roots in ISO 27001/27002. In August 2019, ISO published ISO 27701 as a privacy extension to ISO 27001 and ISO 27002. In Annex 3 of this document, some aspects of the relation between the PCF and ISO's information security and privacy standards will be addressed.

[5] In particular the "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Art. 42 & 43 of the Regulation" and "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)".

9. How the Privacy Control Framework was established

The PCF was built by a working group of NOREA between November 2017 and April 2018. The initial efforts of the working group were further elaborated and structured into version 1.0 of this document, which was peer-reviewed and subsequently approved by NOREA's Professional Practices Committee ("Vaktechnische Commissie"). Version 1.0 was published in May 2018.

In May/June 2019, the PCF was updated and revised to version 2.0, which was peer-reviewed by members of NOREA's Expert Committee Privacy, reviewed and approved by the Professional Practices Committee and published in August 2019.

10. Changes in version 2.0

The following changes were made in updating version 1.0 of the PCF to version 2.0:

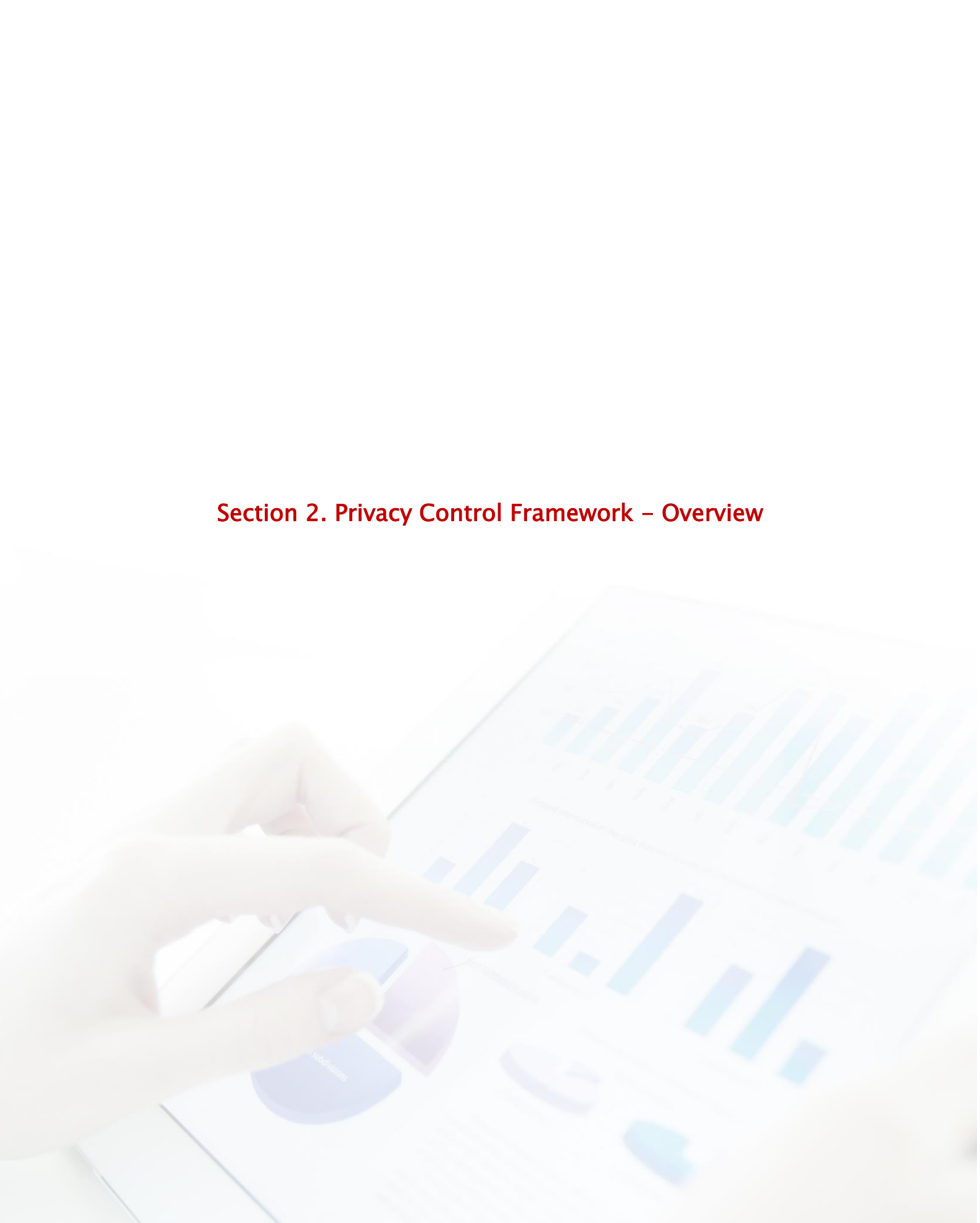
- textual corrections and textual refinements of all sections;
- layout corrections;
- additions in Section1 (subsections 6, 7, 8);
- compression of Annex 1 (PCF-GDPR relation)
- addition of Annex 3 (PCF-ISO relation and cross reference);
- distinction in controls applicable to controllers and processors (section 3);
- establishing a Dutch edition of the PCF.

In comparison with PCF 1.0, there are 9 controls less in PCF 2.0. These controls have been merged with or integrated in other controls, which makes this a reshuffle rather then a change of content. These 'suspended' controls are earmarked as such in section 3.

11. Disclaimer

The PCF is intended to assist IT-auditors, (other) professionals and entities in assessing the system of controls for privacy management. Any results, scoring or recommendations produced on the basis of applying the PCF should not be relied upon in isolation to determine an entity's compliance with GDPR or how GDPR applies to an entity, and the PCF does not constitute legal advice, certifications or guarantees regarding GDPR compliance. The practical application of GDPR is set out in implementation guidelines and regulations. It is expected that these will be further developed (also on the basis of experiences). We encourage all entities using the PCF to also work with a legally qualified professional to monitor GDPR developments, to discuss GDPR and how it applies specifically to their organisation, and how best to ensure compliance.

Section 2. Privacy Control Framework – Overview



The table below summarises the Privacy Control Framework. It contains 95 controls in total, divided over 32 subjects in 9 Lifecycle Management phases. The controls per subject/control objective are listed in detail in Section 3.

Lifecycle phase	Tag	Topic	Control objective	# Controls
Management	PPO	Privacy Policy	The entity establishes and communicates a policy that states its objectives and responsibilities regarding privacy and is in line with accepted privacy principles and applicable laws and regulations.	5
	RRE	Definition of roles and responsibilities	The entity establishes and implements clear roles and responsibilities regarding the safeguarding of personal data and the achievement of privacy objectives.	4
	PDI	Personal Data Identification and classification	The entity understands and documents which personal data is stored and processed and identifies and treats personal data appropriately. Measures to safeguard personal data take into account the differences in sensitivity in personal data, leading to identification of risks and compliance with laws and regulations.	4
	RMA	Risk Management	The entity systematically and periodically identifies, assesses, and mitigates factors that endanger the achievement of privacy objectives.	4
	PIA	Data Protection Impact Assessments	The privacy-related impact of new products and services and their use within the entity is systematically identified, assessed and addressed.	5
	PIB	Privacy Incident and Breach Management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.	8

Lifecycle phase	Tag	Topic	Control objective	# Controls
	SCO	Staff competences	Staff in positions with access to or control over personal data and personal data processes have the necessary privacy competences to adequately perform their duties.	4
	SAT	Staff awareness and training	Staff is sufficiently aware of privacy laws, regulations and organisational privacy policies and guidelines, and their individual responsibilities with regard to privacy, and the entity engages in programs to establish and maintain awareness.	3
	LRC	Legal review of changes in regulatory and/or business requirements	Privacy risks associated with changes to the entity (structure and strategy) and to regulatory requirements are adequately considered.	1
Notice	PST	Privacy statement	The entity transparently informs data subjects of the entity's policy, requirements, and practices regarding the collection, use, retention, disclosure and disposal of personal data.	2
Choice and consent	CFR	Consent framework	The entity obtains data subject's consent for processing personal data where required or necessary.	4
Collect	DMI	Data Minimisation	Personal data is adequate, relevant, and limited to what is necessary in relation to the legitimate purposes for which it is processed.	2
Use, store, and dispose	ULI	Purpose limitation	Personal data is not disclosed, made available or otherwise used for other purposes than those specified in the entity's privacy statement except: a) with the consent of the data subject; or b) by the authority of law.	2
	PBD	Privacy architecture (Privacy by Design	The entity takes into account solid privacy policies, principles, and/or applicable laws and regulations when designing or changing products, services, business systems or processes .	3

Lifecycle phase	Tag	Topic	Control objective	# Controls
		and Privacy by Default)		
	DRE	Data retention	Personal data is retained no longer than the minimum time needed, as required by applicable laws and regulations, or for the purposes for which it was collected.	2
	DDA	Disposal, destruction and anonymisation	Personal data is anonymised and/or disposed of within the entity where required. Identities should not be identifiable and personal data should not be available once it is past its retention date.	2
	URE	Use and restriction	Personal data is not used in case of the restriction of the data subject or in case of specific legal restrictions by local government. Objections to processing by data subject will be handled adequately.	2
Data Access and Data Quality	DAR	Data access requests	Data subject access requests are responded to adequately, and data subjects are able to determine which personal data relating to her/him is processed and in what way.	3
	DCR	Data correction requests	Data subject correction requests are responded to adequately, and data subjects are able to determine whether their personal data is correct/up-to-date, and are able to correct their personal data.	3
	DDR	Data deletion requests	Data deletion requests are responded to adequately and data subjects are able to have their personal data deleted if applicable criteria are met.	3
	DPR	Data portability requests	Data portability requests are responded to adequately and data subjects are able to have their personal data transferred to another entity if applicable criteria are met.	3
	ACD	Accuracy and completeness of data	Documented procedures for validation, editing and update of personal data assure accurate and complete personal data processing.	2

Lifecycle phase	Tag	Topic	Control objective	# Controls
Disclose	TPD	Third party disclosure and registration	Personal data is not disclosed to third parties without a lawful basis or for other purposes than the data subject was informed about.	1
	TPA	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.	3
	DTR	Data Transfers	Personal data is not transferred (i.e. movement, viewing, or printing of data in another location) internationally to countries that have an inadequate legal privacy regime.	2
Data Security	ISP	Information Security Program	Personal data is adequately secured from accidental errors or loss, or from malicious acts such as hacking or deliberate theft, disclosure or loss.	7
	IAM	Identity and access management	Access rights are appropriately assigned, changed and withdrawn, thus decreasing the likelihood of unauthorised access to, or inappropriate handling of personal data, or data breaches by internal employees, third parties or hackers.	1
	STR	Secure transmission	Restricted access to personal data during transmission adequately prevents unauthorised disclosure, breach, altering or destruction of personal data.	1
	ENC	Encryption and end-point security	Encryption assures the prevention of a breach of personal data (accidental loss of personal data, or malicious acts such as deliberate theft, disclosure or loss).	4
	LOG	Logging of access	Access or access attempts to personal data by staff and third parties are logged and investigated to detect and prevent (attempts) to breach security of personal data.	1

Lifecycle phase	Tag	Topic	Control objective	# Controls
Monitoring and enforcement	REV	Review of privacy compliance	Adequate oversight of the internal organisation and third parties ensures compliance with applicable privacy laws and regulatory requirements and decreases the risk of data breaches or loss of personal data.	1
	MON	Periodic monitoring on privacy controls	Systematic and periodical assessments of privacy processes and controls assure that they operate as designed, resulting in ongoing compliance with applicable laws and regulatory requirements.	3

Section 3. Privacy Control Framework – Controls

The following pages contain the PCF's controls per phase in the information lifecycle and per control topic. For each topic, the control objective is listed, as well as the related GDPR key elements.

For each control, a separate column indicates whether that control is applicable for a controlling entity ('C'), a processor ('P'), or both ('C, P').

Management

Privacy Policy (PPO)		
Control objective: The entity establishes and communicates a policy that states its objectives and responsibilities regarding privacy and is in line with accepted privacy principles and applicable laws and regulations.		
Information Lifecycle Management phase: **Management**		
Controls:		
PPO01	A documented privacy policy, which has been communicated to internal personnel and external stakeholders, has been established and is reviewed and approved annually by management.	C, P
PPO02	Management expresses its (responsibility for) commitment to solid and lawful privacy principles.	C, P
PPO03	The privacy policy states the objectives of the entity regarding privacy and personal data protection (see also DMI02, ULI02).	C, P
PPO04	(a) For every instance of processing personal data, the entity establishes alignment with accepted and legal privacy principles, and documents the way in which adherence with these principles is achieved. (b) For every instance of processing personal data, the entity makes sure that documented instructions are in place for each processing activity from contractual partners (controllers or (other) processors)	C P
PPO05	The entity has established and documented the criteria that demonstrate lawful processing for each instance of personal data processing.	C, P
Related GDPR key elements: • Privacy principles • Lawfulness of processing • Records of processing activities		

Definition of roles and responsibilities (RRE)		
Control objective: The entity establishes and implements clear roles and responsibilities regarding the safeguarding of personal data and the achievement of privacy objectives.		
Information Lifecycle Management phase: **Management**		
Controls:		
RRE01	For every personal data processing operation, the entity establishes and documents whether it operates as controller or processor.	C, P
~~RRE02~~	*Replaced by RRE03(b).*	
RRE03	(a) Where the entity operates as a controller, it establishes agreements with processors that govern the privacy responsibilities of the processor. If the entity operates as a joint controller, an arrangement with the other controller is in place. (b) Where the entity operates as a processor, agreements with the controller(s) are in place that govern the privacy responsibilities of the processor. If processing is subcontracted to another processor, agreements are in place that govern the privacy responsibilities of the (sub)controller.	C P
RRE04	The entity assigns coordination, oversight and monitoring of privacy to a designated person, such as a privacy officer or Data Protection Officer (DPO). The responsibility, authority, and accountability of the designated person are clearly documented and regularly reviewed.	C, P
RRE05	The roles and responsibilities of individual staff in safeguarding personal data and compliance with privacy principles are established and communicated.	C, P
Related GDPR key elements: • Privacy principles • Responsibilities of controller and processor • Records of processing activities • Data Protection Officer • Transfers of personal data to third countries or international organisations		

Personal Data Identification and classification (PDI)		
Control objective: The entity understands and documents which personal data is stored and processed and identifies and treats personal data appropriately. Measures to safeguard personal data take into account the differences in sensitivity in personal data, leading to identification of risks and compliance with laws and regulations.		
Information Lifecycle Management phase: **Management**		
Controls:		
PDI01	The entity deploys a documented process to identify and document processing of personal data and classifying that data as such. This includes processes, systems and third parties that handle personal data.	C, P
PDI02	The entity clearly distinguishes and documents processing of (a) personal data and (b) special categories of personal data.	C, P
PDI03	The entity deploys a procedure to assess whether existing or planned processing of personal data involves special categories of personal data. If so, it explicitly assesses and documents the lawfulness of (planned) processing and takes mitigating measures to ensure secure and compliant processing.	P
PDI04	(a) The entity maintains and manages a systematic record of personal data processing activities including the characteristics of these activities (legitimate basis, purpose, categories of data and data subjects, recipients, security measures). (b) The entity maintains and manages a systematic record of personal data processing activities performed on behalf of each controller including the characteristics of these activities (contact details of controller, transfers, security measures).	C P
Related GDPR key elements: • Records of processing activities • Privacy principles • Security of processing		

Risk Management (RMA)		
Control objective: The entity systematically and periodically identifies, assesses, and mitigates factors that endanger the achievement of privacy objectives.		
Information Lifecycle Management phase: **Management**		
Controls:		
RMA01	A process is in place to periodically: a. identify the events and factors endangering privacy objectives; b. assess the impact and probability of these events, and to subsequently formulate adequate risk responses and control measures.	C, P
~~RMA02~~	*Integrated in RMA01.*	
RMA03	When new or changed privacy risks are identified, the privacy risk assessment and the risk response strategies are reviewed and updated where needed.	C, P
RMA04	Privacy risk acceptance criteria are established, approved, documented, and applied.	C, P
RMA05	The entity plans and implements the controls that are necessary to mitigate privacy risk. Progress of implementation is monitored and measured.	C, P
Related GDPR key elements: • Data Protection Impact Assessment • Privacy By Design / by Default		

Data Protection Impact Assessments (PIA) *Control objective:* The privacy-related impact of new products and services and their use within the entity is systematically identified, assessed and addressed.		
Information Lifecycle Management phase: **Management**		
Controls:		
PIA01	The entity deploys a documented process to carry out an assessment of the impact on privacy regarding new or significantly changed processes, products and services (DPIA).	C
PIA02	The DPIA takes into account: a. the envisioned processing operations; b. their purpose, necessity, and proportionality; c. the risks they present to data subject privacy; d. the measures to mitigate these risks.	C
~~PIA03~~	*Integrated with PIA02.*	
PIA04	All relevant stakeholders are involved in the DPIA, and specific guidelines of the supervisory authority regarding assessment criteria are adhered to.	C
PIA05	The entity documents all systems and software that process personal data and a history of changes applied to them.	C
PIA06	A change management process is established to implement approved privacy measures from the DPIA before the change is executed.	C
Related GDPR key elements: • Data Protection Impact Assessment		

Privacy Incident and Breach Management (PIB) *Control objective:* The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.		
Information Lifecycle Management phase: **Management**		
Controls:		
PIB01	A formal, comprehensive privacy incident and breach management process has been implemented, which specifies the following: a. The responsibilities of staff members to inform the responsible privacy officer or DPO in case of a privacy incident or possible data breach; b. The privacy officer or DPO (or, if applicable, security officer) assesses whether the incident is privacy related. In case of a personal data breach, the privacy officer documents the nature of the breach, the consequences, and the approximate number of data records and data subjects affected. c. The privacy officer or DPO initiates and coordinates required actions, and determines the required involvement of individuals and stakeholders to be informed (such as the controller in case the entity is a processor or the supervisory authority if the entity is the controller). d. The privacy officer or DPO monitors the progress of remediating actions and reports to management (and, if applicable, informs the controller and the supervisory authorities).	C, P
~~PIB02~~	*Integrated in PIB06.*	
PIB03	The process includes a clear escalation path, based on the type or severity (or both) of the incident, up to legal counsel and executive management. The process addresses the criteria for contacting law enforcement, regulatory, or other authorities.	C, P
PIB04	(a) The entity has a privacy breach notification policy that ensures that the supervisory authority is timely notified of the data breach if the breach is likely to result in a risk to the rights and freedoms of natural persons. (b) The entity has a privacy breach notification policy that ensures that the respective controller of the processing activity involved is timely notified of a possible data breach.	C P

PIB05	(a) In case of a data breach all required information regarding the breach is collected and provided to the supervisory authority, including cause and mitigating measures. (b) In case of a (possible) data breach all required information regarding the breach is collected and provided to the controller of the processing activity invloved, including cause and mitigating measures.	C P
PIB06	The privacy officer or DPO has been assigned the overall responsibility for the breach notification process. The privacy officer documents all considerations made when determining the obligation to notify.	C, P
PIB07	The breach management process outlines that the evaluation of incidents or breaches leads to remediations and improvements, and serve as input for staff privacy awareness programs.	C, P
PIB08	The privacy incident and breach management process outlines the following: a. after any major privacy incident or data breach, a formal incident evaluation is conducted, where necessary involving external expertise; b. a periodic review of actual incidents is conducted and required improvements are identified based on the following: ○ incident root cause; ○ incident patterns; ○ changes in the internal control environment and legislation; c. results of the periodic review and progress of improvements are reported to and reviewed by management.	C, P
PIB09	The breach management process is reviewed at least every year and shortly after the implementation of significant system or procedural changes.	C, P
Related GDPR key elements: • Personal Data Breach		

Staff competences (SCO)		
Control objective: Staff in positions with access to or control over personal data and personal data processes have the necessary privacy competences to adequately perform their duties.		
Information Lifecycle Management phase: **Management**		
Controls:		
SCO01	The entity documents the required privacy competences for staff that is involved in handling personal data. It also establishes how these competences can be achieved (e.g. training programs).	C, P
SCO02	The entity documents the extent to which individual staff members possess these competences. A process is in place to bridge competence gaps.	C, P
SCO03	The entity addresses privacy competences in its hiring and onboarding process for staff to be involved in safeguarding personal data and compliance with privacy principles, and addresses privacy performance in individual appraisals.	C, P
SCO04	Management annually reviews the allocation of staff, budgets, and other resources to its privacy program.	C, P
Related GDPR key elements: • Security of processing • Privacy principles • Data Protection Officer		

Staff awareness and training (SAT)		
Control objective: Staff is sufficiently aware of privacy laws, regulations and organisational privacy policies and guidelines, and their individual responsibilities with regard to privacy, and the entity engages in programs to establish and maintain awareness.		
Information Lifecycle Management phase: **Management**		
Controls:		
SAT01	A privacy and security awareness course is organised at least annually for all employees. New employees, contractors, and others are required to complete a comparable training within the first month following employment in order to understand the privacy policy of the entity and its implications.	C, P
SAT02	○ In-depth (internal or external) privacy training is provided based on the necessary privacy competences of staff (see SCO). Training covers privacy and relevant security policies and procedures, legal and regulatory considerations, incident response, and related topics. Such training is:required annually for all employees who have access to personal data or are responsible for protection of personal data; ○ tailored to the employee's job responsibilities and required competences.	C, P
SAT03	Training and awareness courses are reviewed and updated to reflect current legislative, regulatory, industry, and entity policy and procedure requirements.	C, P
Related GDPR key elements: • Security of processing • Privacy principles		

Legal review of changes in regulatory and/or business requirements (LRC) *Control objective:* Privacy risks associated with changes to the entity (structure and strategy) and to regulatory requirements are adequately considered.		
Information Lifecycle Management phase: **Management**		
Controls:		
LRC01	The entity establishes a process to monitor, assess, and address the impact on privacy requirements from changes in: a. legal and regulatory requirements; b. industry requirements, best practices and guidelines; c. contracts, including service-level agreements with third parties (changes to the privacy and security related clauses in contracts are adequately reviewed and approved before they are executed); d. business operations and processes; e. people assigned responsibility for privacy and security matters; f. technology (prior to implementation).	C, P
Related GDPR key elements: • Data Protection Impact Assessment • Lawfulness of processing		

Notice

Privacy statement (PST) *Control objective:* The entity transparently informs data subjects of the entity's policy, requirements, and practices regarding the collection, use, retention, disclosure and disposal of personal data.		
Information Lifecycle Management phase: **Notice**		
Controls:		
PST01	The entity's privacy statement: a. describes the personal data obtained, the sources of such information, the purposes for which it is collected and the applicable lawfulness criteria; b. describes the consequences, if any, of the data subject not providing the requested information; c. describes (if applicable) further processing; d. provides information on data subject rights and the procedure to exercise these rights (see also URE, DAR, DCR, DDR, DPR).	C
PST02	The privacy statement is: a. easily accessible and (made) available for data subjects when personal data is first collected from the data subject; b. provided in a timely manner (that is, at or before the time personal data is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal data to the entity; c. clearly dated, to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal data to the entity; d. easily understood and readable.	C
Related GDPR key elements: • Rights of the data subject • Responsibilities of the controller / processor • Privacy principles		

Choice and Consent

Consent framework (CFR) *Control objective:* The entity obtains data subject's consent for processing personal data where required or necessary.		
Information Lifecycle Management phase: **Choice and consent**		
Controls:		
CFR01	The entity's privacy statement describes, in a clear and concise manner, the following: a. the choices available to the data subject regarding the collection, use, and disclosure of personal data; b. the process a data subject should follow to exercise these choices (for example, checking an opt out box to decline receiving marketing materials); c. the ability of, and process for, an individual to change contact preferences; d. the consequences of failing to provide personal data required for a transaction or service; e. the consequences of refusing to provide personal data (for example, transactions may not be processed); f. the consequences of denying or withdrawing consent (for example, opting out of receiving information about products and services may result in not being made aware of sales promotions).	C
CFR02	If processing is based on data subject's consent, the entity: a. obtains and documents a data subject's consent in a timely manner (that is, at or before the time personal data is collected or soon after); b. confirms an individual's preferences (in writing or electronically); c. documents and manages changes to an individual's preferences; d. ensures that an individual's preferences are implemented in a timely fashion; e. retains information to be able to demonstrate given consent.	C
CFR03	The entity does not collect or process special categories of personal data, unless it has a lawful basis to do. If explicit consent of the data subject is the lawful basis for processing special categories of personal data, the data subject has affirmatively agreed, through some action, to the use or disclosure of the special categories of personal data. The entity obtains explicit consent directly	C

	from the data subject and documents/retains evidence of the data subject's consent, for example, by requiring the individual to check a box or sign a form.	
CFR04	In case of processing of personal data on the basis of data subject's consent, the entity will facilitate the data subject in exercising its right to withdraw consent at any time.	C
Related GDPR key elements: • Lawfulness of processing • Conditions for consent • Rights of the data subject		

Collect

Data Minimisation (DMI) *Control objective:* Personal data is adequate, relevant, and limited to what is necessary in relation to the legitimate purposes for which it is processed.		
Information Lifecycle Management phase: **Collect**		
Controls:		
DMI01	The entity establishes a process and procedures to: a. identify the extent to which personal data is essential for the purposes of the entity's processing, and to differentiate it from optional personal data; b. limit processing of personal data to the minimum extent required by the processing purposes; c. periodically review the continuing necessity of personal data in the entity's products and/or services.	C
DMI02	The privacy policy states data minimisation as a privacy principle for the entity (see PPO).	C
Related GDPR key elements: • Privacy principles • Privacy By Design / by Default		

Use, store and dispose

Purpose limitation (ULI) *Control objective:* Personal data is not disclosed, made available or otherwise used for other purposes than those specified in the entity's privacy statement except: a) with the consent of the data subject; or b) by the authority of law.		
Information Lifecycle Management phase: **Use, store and dispose**		
Controls:		
ULI01	The entity establishes a process and procedures to: a. limit disclosure and use of personal data to the legitimate purposes as documented in the entity's privacy policy and privacy statement; b. continuously assure that disclosure and use of personal data in agreement with the data subject's consent and applicable laws and regulations.	C
ULI02	The privacy policy states purpose limitation as a privacy principle for the entity (see PPO).	C
Related GDPR key elements: • Privacy principles • Privacy By Design / by Default		

Privacy architecture (Privacy by Design and Privacy by Default) (PBD) *Control objective:* The entity takes into account solid privacy policies, principles, and/or applicable laws and regulations when designing or changing products, services, business systems or processes .		
Information Lifecycle Management phase: **Use, store and dispose**		
Controls:		
PBD01	When developing, designing, selecting and using applications, services and products that process personal data, the entity takes into account the privacy principles and privacy risks as early as possible in the design phase. The risk of conflicts between the privacy design and the rights and freedoms of data subjects (and the entity's privacy policy) is identified and addressed. If the entity procures services of third parties in these activities, it will require these third parties to deploy the same privacy risk management activities.	C
PBD02	Assessment of privacy risks is an inherent and documented element of the entity's project methodology and/or design and development process.	C
PBD03	Where the systems, services and products that process personal data offer privacy-related choices and options, the default setting for these choices and options will be as restrictive as possible in terms of privacy.	C
Related GDPR key elements: • Privacy by Design / by Default • Privacy principles		

Data retention (DRE) *Control objective:* Personal data is retained no longer than the minimum time needed, as required by applicable laws and regulations, or for the purposes for which it was collected.		
Information Lifecycle Management phase: **Use, store and dispose**		
Controls:		
DRE01	The entity: a. documents its retention policies and disposal procedures for personal data; b. ensures personal data is not kept beyond the established retention time unless a justified business or legal reason for doing so exists; c. for each instance of personal data processing, documents applicable retention times; d. discloses retention time policies to data subjects in its privacy statement; e. retains, stores, and disposes archived and backup copies of records in accordance with its retention policies; f. instructs processor(s) regarding data retention (periods)	C
DRE02	Legal and contractual retention requirements are considered when establishing retention practices when they may be exceptions to normal policies.	C
Related GDPR key elements: • Privacy principles • Responsibilities of the controller / processor		

Disposal, destruction and anonymization (DDA) *Control objective:* Personal data is anonymised and/or disposed of within the entity where required. Identities should not be identifiable and personal data should not be available once it is past its retention date.		
Information Lifecycle Management phase: **Use, store and dispose**		
Controls:		
DDA01	The entity has a documented process in place that ensures: a. erasure or destruction of personal data records in accordance with the retention policies, regardless of the nature of storage media (for example, electronic, optical media, or paper based); b. disposal of original, archived, backup and ad hoc or personal copies of records in accordance with its destruction policies; c. adequate documentation of the disposal of personal data. The entity further: d. within the limits of technology, locates and removes or reduces specified personal data about an individual as required; e. regularly and systematically destroys, erases, or anonymises personal data that is no longer required to fulfill the identified purposes or as required by laws and regulations.	C
DDA02	Contractual requirements are considered when establishing disposal, destruction, and reduction practices if they may result in an exception to the entity's normal policies.	C
Related GDPR key elements: • Privacy principles • Responsibilities of the controller / processor • Security of processing • Privacy By Design / by Default		

Use and restriction (URE) *Control objective:* Personal data is not used in case of the restriction of the data subject or in case of specific legal restrictions by local government. Objections to processing by data subject will be handled adequately.		
Information Lifecycle Management phase: **Use, store and dispose**		
Controls:		
~~URE01~~	*Integrated in PST01*.	
URE02	The entity has a process in place to adequately respond to data subjects exercising their rights to restriction of processing or to object to processing.	C
URE03	The entity has established whether local member state law imposes any restrictions on personal data processing (e.g. to safeguard national or public security) and is demonstrably compliant with these restrictions.	C
Related GDPR key elements: • Privacy principles • Lawfulness of processing • Rights of the data subject • Transfers of personal data to third countries or international organisations		

Data access and data quality

Data access requests (DAR) *Control objective:* Data subject access requests are responded to adequately, and data subjects are able to determine which personal data relating to her/him is processed and in what way.		
Information Lifecycle Management phase: **Data access and data quality**		
Controls:		
DAR01	Procedures are in place to adequately respond to data subject access requests. In case the data subject exercises his/her right, the entity will inform the data subject of the nature of the personal data it processes and the characteristics of the processing (e.g. purpose, recipients, retention times, the existence of automated decision making).	C
~~DAR02~~	*Integrated in PST01.*	
DAR03	The entity has a process in place to timely provide to the data subject, in a commonly used electronic form, a copy of the personal data undergoing processing.	C
DAR04	The entity verifies the identity of the requesting data subject before responding.	C
Related GDPR key elements: • Security of processing • Privacy by Design / by Default • Rights of the data subject		

Data correction requests (DCR) *Control objective:* Data subject correction requests are responded to adequately, and data subjects are able to determine whether their personal data is correct/up-to-date and are able to correct their personal data.		
Information Lifecycle Management phase: **Data Access and data quality**		
Controls:		
DCR01	Procedures are in place to adequately respond to data subject correction requests. In case the data subject exercises this right, the entity will rectify the personal data of the data subject without undue delay.	C
~~DCR02~~	*Integrated in PST01.*	
DCR03	The entity verifies the identity of the requesting data subject before acting on the request.	C
DCR04	The entity notifies third parties, to whom personal data has been disclosed, of necessary corrections in personal data.	C
Related GDPR key elements: • Rights of the data subject		

Data deletion requests (DDR)		
Control objective: Data deletion requests are responded to adequately and data subjects are able to have their personal data deleted if applicable criteria are met.		
Information Lifecycle Management phase: **Data Access and data quality**		
Controls:		
DDR01	Procedures are in place to adequately respond to data subject deletion requests ('right to be forgotten'). In case the data subject exercises his/her right, the entity will validate the grounds of the request against applicable criteria (e.g. processing is consent-based, unlawful processing, purpose no longer valid, legal requirements for retention). Where a valid ground exists, the entity will erase the personal data without undue delay.	C
DDR02	If applicable, the entity notifies other controllers, to whom the personal data has been passed on, of the data subject's request to have personal data deleted. If the personal data are processed by a processor, the entity instructs the processor to delete the data.	C
~~DDR03~~	*Integrated in PST01*.	
DDR04	The entity verifies the identity of the requesting data subject before acting on the request.	C
Related GDPR key elements: • Rights of the data subject		

Data portability requests (DPR) *Control objective:* Data portability requests are responded to adequately and data subjects are able to have their personal data transferred to another entity if applicable criteria are met.		
Information Lifecycle Management phase: **Data Access and data quality**		
Controls:		
DPR01	Procedures are in place to adequately respond to data subject portability requests. In case the data subject exercises his/her right, the entity will validate the grounds of the request against applicable criteria (e.g. processing is consent-based, processing is carried out by automated means). Where a valid ground exists, the entity will transfer the personal data without undue delay.	C
DPR02	If technically feasible, the entity will transfer the personal data directly to another (controlling) entity as instructed by the data subject.	C
~~DPR03~~	*Integrated in PST01*.	
DPR04	The entity verifies the identity of the requesting data subject before acting on the request.	C
Related GDPR key elements: • Rights of the data subject • Right to data portability		

Accuracy and completeness of data (ACD) *Control objective:* Documented procedures for validation, editing and update of personal data ensure accurate and complete personal data processing.		
Information Lifecycle Management phase: **Data Access and data quality**		
Controls:		*Evidence/testing:*
ACD01	The entity has procedures in place to: a. edit and validate personal data as it is collected, created, maintained, and updated; b. record the date when the personal data is obtained or updated; c. specify when the personal data is no longer valid; d. specify when and how the personal data is to be updated and the source for the update (for example, annual reconfirmation of information held and methods for individuals to proactively update personal data); e. indicate how to verify the accuracy and completeness of personal data obtained directly from an individual, received from a third party, or disclosed to a third party; f. ensure personal data processed is sufficiently accurate and complete to make decisions.	C
ACD02	The entity undertakes periodic assessments to check the accuracy of personal data records and to correct them, as necessary, to fulfill the stated purpose.	C
Related GDPR key elements: • Security of processing		

Disclose

Third party disclosure and registration (TPD) *Control objective:* Personal data is not disclosed to third parties without a lawful basis or for other purposes than the data subject was informed about.		
Information Lifecycle Management phase: **Disclose**		
Controls:		
TPD01	The entity has procedures in place to: g. prevent the disclosure of personal data to third parties if there is no lawful basis to do so and/or the data subject has not been informed; h. document the nature and extent of personal data disclosed to third parties; i. monitor whether disclosure to third parties is in continuous compliance with the entity's privacy policies and procedures, or is specifically allowed or required by law or regulation; j. document any third-party disclosures for legal reasons; k. notify data subjects and obtain their consent prior to disclosing personal data to a third party for purposes not identified in the privacy notice; l. monitor that personal data is only provided to third parties for purposes specified in the privacy notice.	C
Related GDPR key elements: • Security of processing • Lawfulness of processing		

Third party agreements (TPA) *Control objective:* Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.		
Information Lifecycle Management phase: **Disclose**		
Controls:		
TPA01	(a) If the entity procures solutions from third parties/suppliers or outsources processes to service providers, and processing of personal data is (partially) contracted, the entity enters into formal agreements that require from the third party due care and a level of protection of personal data equivalent to that of the entity. In doing so, the entity limits the third party's use of personal data to purposes established by the entity. (b) The entity ensures that subcontracting the processing of personal data to another processor is only done after prior authorisation of the controller. If the controller approves, the entity enters into formal agreements that require from the third party due care and a level of protection of personal data equivalent to that of the entity.	C P
TPA02	The entity ensures that the agreements will also address the following obligations of the third party: m. confidentiality and non-disclosure; n. security requirements; o. cooperation in responding to data subject requests and data subject rights execution; p. information provision (e.g. in case of planned subcontracting); q. information provision and cooperation in case of data breaches; r. retention periods and data deletion; s. no further subcontracting without permission of the entity; t. liabilities and indemnifications.	C, P
TPA03	The entity evaluates the performance and compliance of third parties using one or more of the following approaches (in ascending order of assurance and depending on the risk profile of the third party): a. the third party responds to a questionnaire about its practices; b. the third party self-certifies that its practices meet the entity's requirements based on internal audit reports or other procedures;	C, P

	c. the entity performs a periodic on-site evaluation of the third party; d. The entity engages in an audit or assurance assessment provided by an independent auditor.	
Related GDPR key elements: • Responsibilities of controller / processor • Security of processing		

Data Transfers (DTR)		
Control objective: Personal data is not transferred (i.e. movement, viewing, or printing of data in another location) internationally to countries that have an inadequate legal privacy regime.		
Information Lifecycle Management phase: **Disclose**		
Controls:		*Evidence/testing:*
DTR01	The entity has established any instances where personal data under its responsibility is being transferred to and processed in third countries that possibly insufficiently guarantee the privacy rights of data subjects.	C, P
DTR02	The entity only transfers personal data to third countries, for which (a) an Adequacy Decision from the European Commission has been issued, or (b) a set of appropriate safeguards (e.g. binding corporate rules or adopted standard data protection clauses) has been implemented.	C, P
Related GDPR key elements: • Transfers of personal data to third countries or international organisations		

Data Security

Information Security Program (ISP) *Control objective:* Personal data is adequately secured from accidental errors or loss, or from malicious acts such as hacking or deliberate theft, disclosure or loss.		
Information Lifecycle Management phase: **Data security**		
Controls:		
ISP01	The entity has taken appropriate technical and organisational measures to ensure security of personal data. Security comprises confidentiality, integrity, and availability of personal data. Also refer to IAM, STR, ENC, LOG.	C, P
ISP02	Security of personal data is explicitly addressed in the entity's information security policies and the information security management system.	C, P
ISP03	The appropriateness of security measures regarding personal data is established in periodic risk assessments in which all relevant stakeholders take part and in which actual and planned personal data processing is assessed.	C, P
ISP04	The entity has a documented policy on encryption and pseudonymisation of personal data and systematically verifies adherence to the policy (also refer to ENC).	C, P
ISP05	The entity regularly tests, assesses and evaluates the effectiveness of technical and organisational security measures to ensure an adequate level of personal data security and to identify and initiate improvements.	C, P
ISP06	The entity has an active stance towards deploying a code of conduct (from associations or industry bodies) and/or certifications to demonstrate an appropriate level of personal data security.	C, P
ISP07	The entity's security program prevents access to personal data in computers, media, and paper-based information that are no longer in active use by the organisation (for example, computers, media, and paper-based information in storage, sold, or otherwise disposed of).	C, P
Related GDPR key elements: • Security of processing		

Identity and access management (IAM) *Control objective:* Access rights are appropriately assigned, changed and withdrawn, thus decreasing the likelihood of unauthorised access to, or inappropriate handling of personal data, or data breaches by internal employees, third parties or hackers.		
Information Lifecycle Management phase: **Data security**		
Controls:		
IAM01	Systems and procedures are in place to: a. establish the level and nature of access that will be provided to users, based on the sensitivity of the personal data and the user's legitimate business needs to access the personal data; b. identify and authenticate users, for example, by user name and password, certificate, external token, or biometrics before access is granted to systems handling personal data; c. require enhanced security measures for remote access, such as additional or dynamic passwords, callback procedures, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls; d. implement intrusion detection and monitoring systems.	C, P
Related GDPR key elements: • Security of processing		

Secure transmission (STR) *Control objective:* Restricted access to personal data during transmission adequately prevents unauthorised disclosure, breach, altering or destruction of personal data.		
Information Lifecycle Management phase: **Data security**		
Controls:		
STR01	Systems and procedures are in place to: a. define minimum levels of security for transmission of personal data; b. employ industry standard encryption technology for transfer and receipt of personal data; c. assess and approve external network connections; d. protect personal data in both hardcopy and electronic forms sent by mail, courier, or other physical means; e. encrypt personal data collected and transmitted wirelessly and protect wireless networks from unauthorized access.	C, P
Related GDPR key elements: • Security of processing • Personal Data Breach		

Encryption and end-point security (ENC) *Control objective:* Encryption assures the prevention of a breach of personal data (accidental loss of personal data, or malicious acts such as deliberate theft, disclosure or loss).		
Information Lifecycle Management phase: **Data security**		
Controls:		
ENC01	Policies and procedures prohibit the storage of personal data on portable media or devices unless a business need exists and such storage is approved by management.	C, P
ENC02	Policies, systems, and procedures are in place to protect personal data accessed or stored on devices such as: a. laptop computers, PDAs, smart- phones and similar devices; b. computers and other devices used by employees while, for example, traveling and working at home; c. USB drives, CDs and DVDs, magnetic tape, or other portable media. Such information is encrypted, password protected, physically protected, and subject to the entity's access, retention and destruction policies.	C, P
ENC03	Procedures and systems exist for creation, transfer, storage, and disposal of media containing personal data used for backup and recovery.	C, P
ENC04	Procedures exist to report loss or potential misuse of media containing personal data (also refer to PIA). Upon termination of employee- or third-party contracts, procedures provide for the return or destruction of portable media and devices used to access and store personal data, and of printed and other copies of such information.	C, P
Related GDPR key elements: • Security of processing • Personal Data Breach		

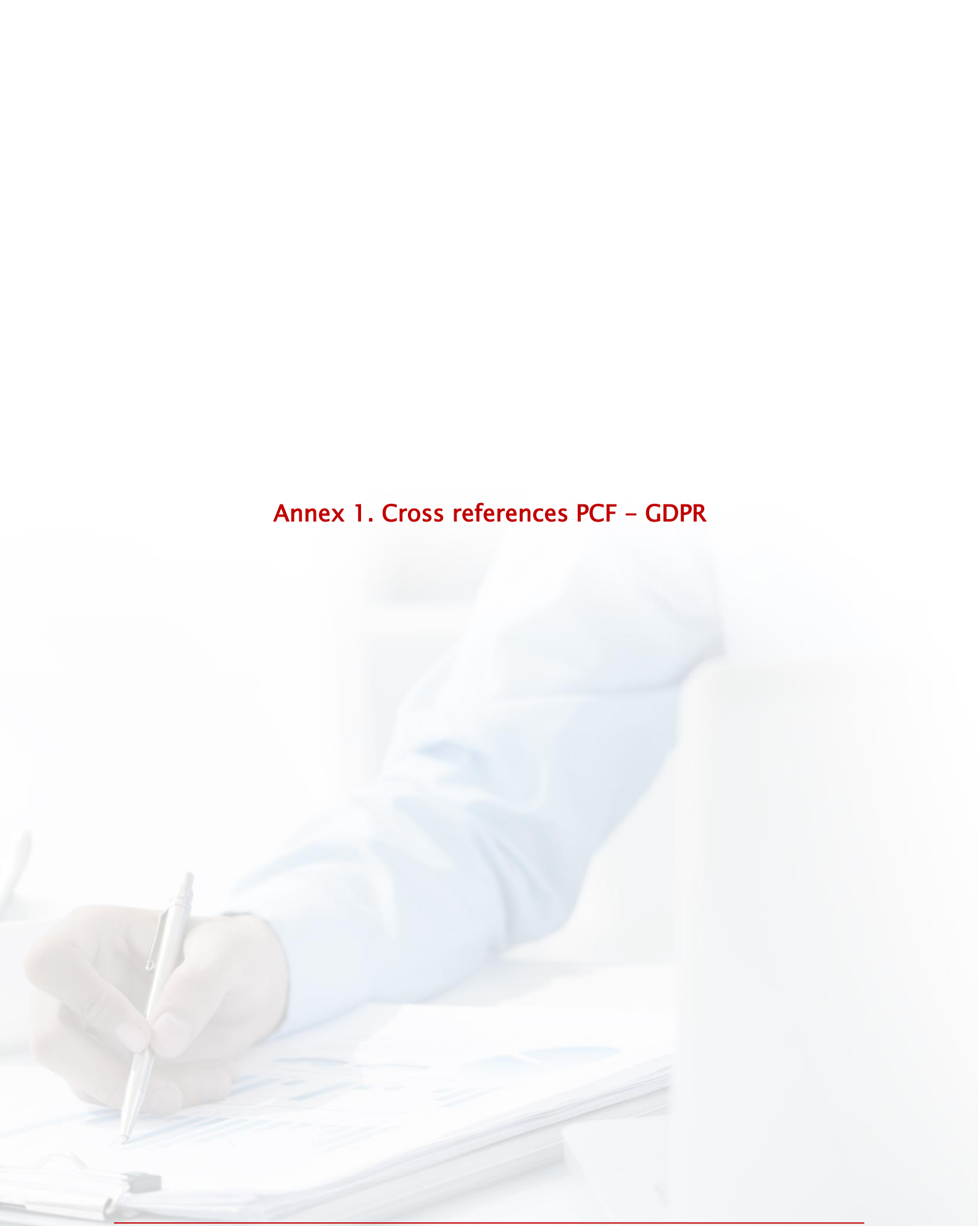
Logging of access (LOG) *Control objective:* Access or access attempts to personal data by staff and third parties are logged and investigated to detect and prevent (attempts) to breach security of personal data.		
Information Lifecycle Management phase: **Data security**		
Controls:		
LOG01	Systems and procedures are in place to: a. manage logical and physical access to personal data, including hard copy, archive- and backup copies; b. log and monitor access (attempts) to systems with personal data in a logfile with a level of detail and retention time sufficient for the purposes of analysis and investigation; c. prevent the unauthorised or accidental destruction or loss of personal data; d. investigate breaches and attempts to gain unauthorized access.	C, P
Related GDPR key elements: • Security of processing • Personal Data Breach		

Monitoring and Enforcement

Review of privacy compliance (REV) *Control objective:* Adequate oversight of the internal organisation and third parties ensures compliance with applicable privacy laws and regulatory requirements and decreases the risk of data breaches or loss of personal data.		
Information Lifecycle Management phase: **Monitoring and enforcement**		
Controls:		
REV01	Systems and procedures are in place to: a. annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service level agreements, standards adopted by the entity, and other contracts; b. document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign-offs; c. report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan; d. monitor the resolution of issues and vulnerabilities noted in the compliance review to ensure that appropriate corrective action is taken on a timely basis (including revision of privacy policies and procedures, where necessary).	C, P
Related GDPR key elements: • Lawfulness of processing		

Periodic monitoring on privacy controls (MON) *Control objective:* Systematic and periodical assessments of privacy processes and controls assure that they operate as designed, resulting in ongoing compliance with applicable laws and regulatory requirements.		
Information Lifecycle Management phase: **Monitoring and enforcement**		
Controls:		
MON01	Management of the entity reviews the following to ensure operational effectiveness of privacy controls: a. control outputs, control reports and deviations; b. trend analysis; c. training attendance and evaluations; d. complaints and their resolutions; e. internal reviews; f. internal and external audit reports; g. independent audit/assurance reports covering privacy controls at service organisations; h. other evidence of control effectiveness.	C, P
MON02	The selection of controls to be monitored, reviewed and/or audited and the frequency and extent with which this is performed are based on the sensitivity of the personal data involved and the risks of possible exposure or loss.	C, P
MON03	The entity deploys a process that ensures that monitoring leads to remediation of shortcomings and continuous improvement.	C, P
Related GDPR key elements: • Lawfulness of processing		

Annex 1. Cross references PCF – GDPR



Cross reference of GDPR key elements with GDPR articles

The following table shows the relation between GDPR key elements, the articles in the GDPR, and the PCF topics.

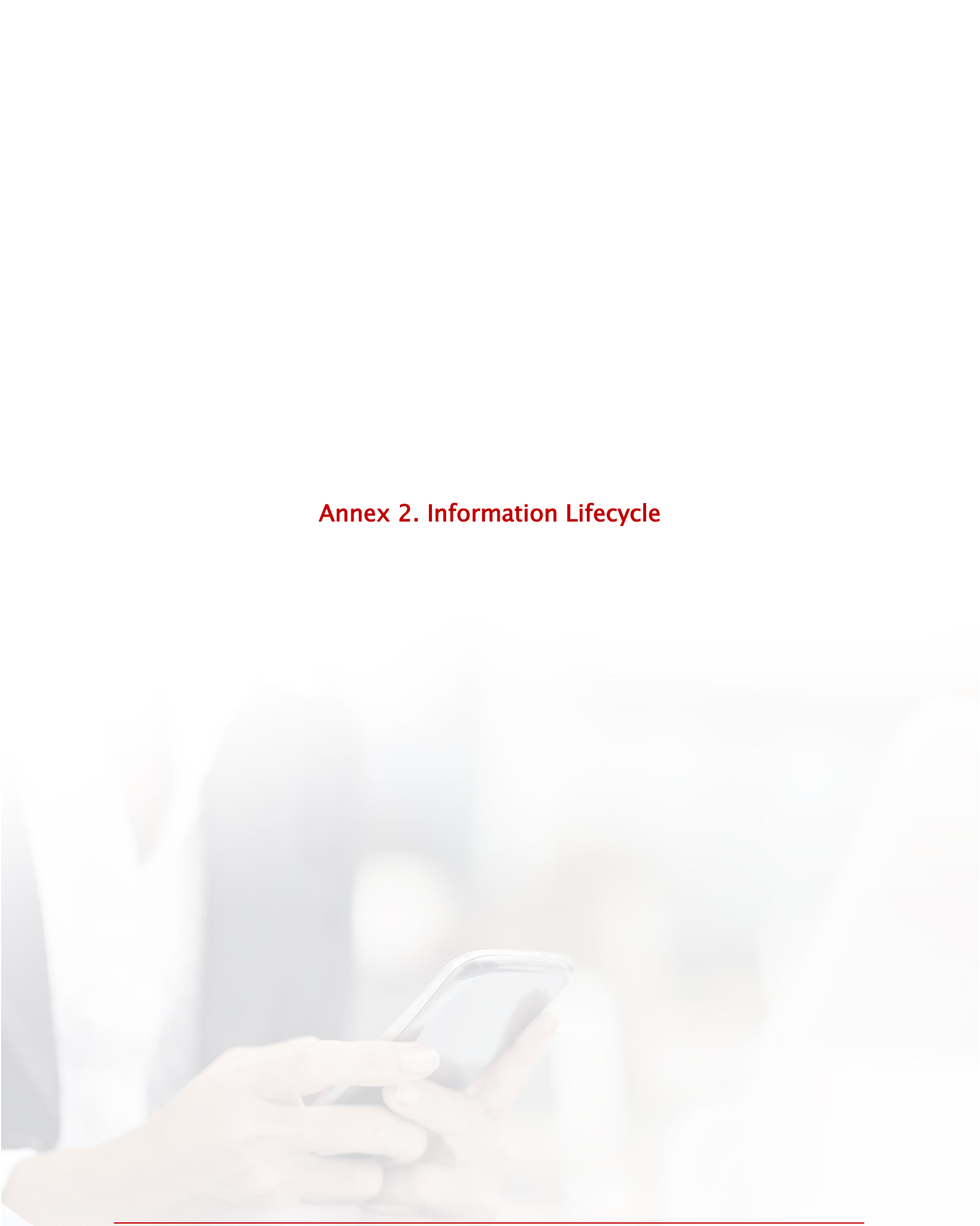
GDPR key element	Related GDPR Articles	Cross-reference to PCF Topic
Privacy Principles	Article 5 – Principles relating to processing of Personal data	• Privacy Policies (PPO) • Definition of roles and responsibilities (RRE) • Staff competences (SCO) • Personal Data Identification and classification (PDI) • Staff awareness and training (SAT) • Purpose limitation (ULI) • Privacy statement (PST) • Data Minimisation (DMI) • Purpose limitation (ULI) • Privacy architecture (Privacy by Design and Privacy by Default) • Data retention (DRE) • Disposal, destruction and anonymisation (DDA) • Use and restriction (URE)
Lawfulness of Processing	Article 6 – Lawfulness of processing	• Privacy Policy (PPO) • Consent framework (CFR) • Legal review of changes in regulatory and/or business requirements (LRC) • Use and restriction (URE) • Third party disclosure and registration (TPD) • Review of privacy compliance (REV) • Periodic monitoring on privacy controls (MON)
Conditions for Consent	Article 7 – Conditions for consent	• Privacy Policy (PPO) • Consent framework (CFR) • Legal review of changes in regulatory and/or business requirements (LRC)

GDPR key element	Related GDPR Articles	Cross-reference to PCF Topic
		• Use and restriction (URE) • Third party disclosure and registration (TPD) • Review of privacy compliance (REV) • Periodic monitoring on privacy controls (MON)
Rights of the data subject	Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject Article 13 – Information to be provided where personal data are collected from the data subject Article 14 – Information to be provided where personal data have not been obtained from the data subject Article 15 – Right of access by the data subject Article 16 – Right to rectification Article 17 – Right to erasure ('right to be forgotten') Article 18 – Right to restriction of processing Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing Article 20 – Right to data portability	• Use and restriction (URE) • Data access requests (DAR) • Consent framework (CFR) • Privacy statement (PST) • Data correction requests (DCR) • Data deletion requests (DDR)
Right to data portability	Article 20 – Right to data portability	• Data portability requests (DPR)
Privacy By Design / by Default	Article 25 – Data protection by design and by default	• Risk Management (RMA) • Definition of roles and responsibilities (RRE) • Staff competences (SCO) • Data Minimisation (DMI)

GDPR key element	Related GDPR Articles	Cross-reference to PCF Topic
		• Purpose limitation (ULI) • Privacy architecture (Privacy by Design and Privacy by Default) (PBD) • Data access requests (DAR) • Disposal, destruction and anonymisation (DDA)
Responsibilities of controller and processor	Article 24 – Responsibility of the controller Article 28 – Processor	• Definition of roles and responsibilities (RRE) • Privacy statement (PST) • Data retention (DRE) • Disposal, destruction and anonymisation (DDA) • Third party agreements (TPA)
Records of processing activities	Article 30 – Records of processing activities	• Privacy Policy (PPO) • Definition of roles and responsibilities (RRE) • Personal Data Identification and classification (PDI)
Security of processing	Article 32 – Security of Processing	• Personal Data Identification and classification (PDI) • Staff competences (SCO) • Staff awareness and training (SAT) • Definition of roles and responsibilities (RRE) • Disposal, destruction and anonymisation (DDA) • Data access requests (DAR) • Accuracy and completeness of data (ACD) • Third party disclosure and registration (TPD) • Third party agreements (TPA) • Information Security Program (ISP) • Identity and access management (IAM) • Secure transmission (STR) • Encryption and end-point security (ENC)

GDPR key element	Related GDPR Articles	Cross-reference to PCF Topic
		• Logging of access (LOG) •
Personal Data Breach	Article 33 – Notification of a personal data breach to the supervisory authority Article 34 – Communication of a personal data breach to the data subject	• Privacy Incident and Breach Management (PIB) • Secure transmission (STR) • Encryption and end-point security (ENC) • Logging of access (LOG)
Data Protection Impact Assessment (DPIA)	Article 35 – Data Protection Impact Assessment	• Risk Management (RMA) • Data Protection Impact Assessments (PIA) • Legal review of changes in regulatory and/or business requirements (LRC)
Data Protection Officer (DPO)	Article 37 – Designation of the data protection officer Article 38 – Position of the data protection officer Article 39 – Tasks of the data protection officer	• Definition of roles and responsibilities (RRE) • Staff competences (SCO)
Transfers of personal data to third countries or international organisations	Article 44 – General principle for transfers Article 45 – Transfers on the basis of an adequacy decision Article 46 – Transfers subject to appropriate safeguards Article 47 – Binding corporate rules Article 48 – Transfers or disclosures not authorised by Union law Article 49 – Derogations for specific situations Article 50 – International cooperation for the protection of personal data	• Definition of roles and responsibilities (RRE) • Use and restriction (URE) • Data Transfers (DTR)

Annex 2. Information Lifecycle



Introduction

This Annex gives a description of the essentials of the information lifecycle model as stated in section 1 – Introduction.

The PCF is structured along an Information lifecycle model, which was first outlined by Koetsier and Ougajou in their thesis and subsequent publication in "De IT-auditor".

A graphical representation of the information lifecycle model will be given in the next figure:

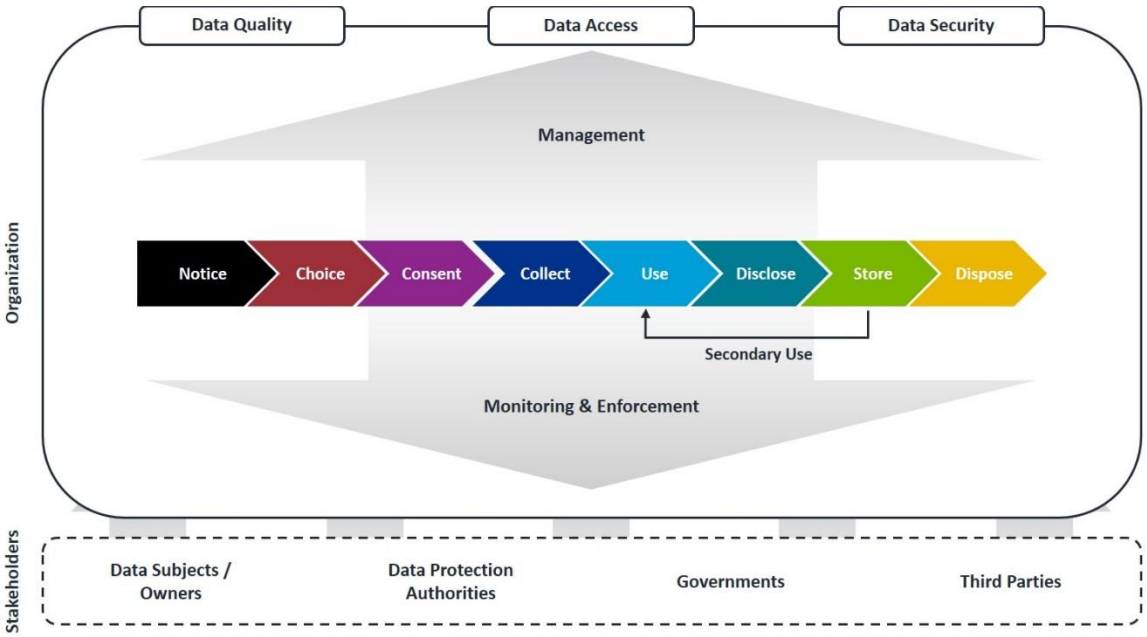


Figure 1 Information Lifecycle Model

Different Phases

The information life cycle model has been based and defined upon a mix of GAPP[6]-principles and OECD-[7]principles. The Information lifecycle model consists of 8 different phases:

1. **Notice**: The information lifecycle starts with informing the data subject about the usage of his personal data . The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

2. **Choice**: The entity describes the different choices available to the data subject with respect to the collection, use, and disclosure of personal information by the entity.

3. **Consent**: The entity secures implicit or explicit consent of the data subject regarding the collection, use and disclosure of the personal data.

4. **Collect**: Personal information is only collected by the entity for the purposes identified in the phase Notice.

5. **Use**: The entity limits the use of personal information to the purposes identified in the phase Notice and for which the data subject has provided implicit or explicit consent.

6. **Disclose**: The entity discloses personal information to third parties only for the purposes identified in the phase Notice and with the implicit or explicit consent of the data subject.

7. **Store**: The entity stores personal information not longer than needed related to the purpose as defined in the phase Notice or as required by laws and regulations. There is a possibility that personal data will be re-used ('secondary use') and flows back to the phase Use, only if the purposes for secondary use are in line with those communicated in the phase Notice.

8. **Dispose**: The entity appropriately disposes personal information.

---

[6] GAPP, An Executive Overview of GAPP: Generally Accepted Privacy Principles, 2009.

[7] The OECD Privacy Framework, Organisation for Economic Co-operation and Development, 2013.

Preconditions - management and stakeholders

Management determines the direction (e.g. privacy strategy, privacy policy, etc.) and ensures that personal data flows through the different phases of the information lifecycle in a controlled manner (monitoring and enforcement). In general, there are three preconditions for personal data in the various phases of the information lifecycle to ensure business processes operate in an accurate, complete and timely manner:

- Data quality;
- Data access;
- Data security.

Finally, the information lifecycle model also presents the various external stakeholders with regard to the different phases in the processing of personal data. This stakeholders concerns:

- Data subjects;
- Data Protection Authorities (e.g. the Autoriteit Persoonsgegevens in the Netherlands);
- Governments;
- Third parties (or data processors).

Based on this conceptual model the PCF has been developed, which includes an overview of control objectives and corresponding control measures. The control objectives are grouped according to the different phases mentioned in the information lifecycle model.

This provides a clear overview of the various privacy control objectives positioned in the phases of the information lifecycle model. By using this model, governance of personal data in entities can be significantly improved.

Annex 3. PCF and ISO Standards

This annex provides clarification regarding the relation between the PCF and:

- ISO 27001/27002 (in this annex referred to as 'ISO 27001')[8]
- ISO 27701
- ISO 29100

ISO 27001/27002 and privacy

The terms 'privacy' and 'personal data' are scarcely mentioned in ISO 27001. That is not surprising, as ISO 27001 is aimed at information security in general, in which nature and classification of information to be protected should be taken into account. Personal data are thus implicitly included in ISO 27001. In the ISO 27001 controls, personal data are explicitly mentioned in one control only. A.18.1.4 (in chapter "Compliance" of Annex A) states as objective:

"Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable."

This, in fact, implies that ISO 27001 not only requires adequate protection of personal data, but also compliance with the GDPR. In this line of reasoning, it could be defended that compliance with ISO 27001 requirements implies sufficient control regarding security of personal data and compliance with privacy laws and regulations. Theoretically, the PCF can be used to establish whether control A.18.1.4 has been adequately designed and operates effectively. The plausibility of such an approach is questionable. It requires the PCF's 32 control objectives to be 'added' to ISO 27001 to establish achievement of *one* ISO 27001 control objective.

A more practical way in which ISO 27001 and PCF can co-exist is to regard PCF's privacy related controls as an 'extension for personal data' of various individually required information security controls in ISO 27001. By doing so, the PCF is virtually 'spread out' over ISO 27001 in stead of being linked to the individual requirement A.18.1.4. Professionals would then use the PCF as a privacy related addendum on top of ISO 27001, taking into account personal data as a specific occurrence of information, the protection of which demands requirements that are privacy specific extensions of existing ISO 27001 controls. To illustrate this, the example below links ISO 27001 A.16 (Incident Management) to PCF PIB (Privacy incident and breach Management).

[8] NEN-ISO/IEC 27001 is an information security standard that specifies requirements of an information security management system (ISMS). ISO/IEC 27002 provides best practice recommendations on information security controls for use in an ISMS, using the same objectives as ISO 27001.

	ISO 27001 – ISMS	PCF – Privacy specific
Topic/onderdeel	**A.16** Incident Management	**PIB** – Privacy Incident & Breach Management
Control objective	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	The entity adequately detects and handles privacy related incidents. Privacy-related incidents are responded to appropriately as to limit the consequences and take measures to prevent future breaches.
Control	**A.16.1.2** Information security events shall be reported through appropriate management channels as quickly as possible.	**PIB03** The process includes a clear escalation path, based on the type or severity, or both, of the incident, up to legal counsel and executive management. The process addresses the criteria for contacting law enforcement, regulatory, or other authorities.

When using this approach, it is helpful to use a mapping which links controls from ISO 27001 and PCF (analogous to what was done in the above example for A.16.1.2 (ISO 27001) and PIB (PCF)). Such a(n illustrative) cross-reference is listed in the table at the end of this annex, to support professionals who use the PCF in an entity where ISO 27001 is already deployed as a normative framework for information security.

ISO 27701

ISO as an organisation also seems to favour the approach as described. In August 2019 it published ISO/IEC 27701:2019 (in short: ISO 27701), which is a privacy extension to the requirements and guidance in ISO 27001 and ISO 27002 respectively. The full title of the standard is 'Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.'

In short, ISO 27701 provides privacy additions and refinements to existing clauses and requirements of ISO 27001 and to guidance from ISO 27002. Whereas ISO 27001 and ISO 27001 are aimed at (requirements for) an information security management system (ISMS), ISO 27701 enhances this with requirements regarding a privacy information management system (PIMS). Based on ISO 27701, the PIMS of an organisation can be designed, implemented, and certified.

One of ISO 27701's annexes provides an extensive cross reference between the requirements of ISO 27701 and the related articles in the GDPR.

ISO 29100

To complete the picture, we mention ISO/IEC 29100:2011 "Information technology – Security techniques – Privacy framework" (in short: ISO 29100) as another ISO standard that is specifically aimed at privacy. This standard provides the outlines for a high-level privacy framework, which supports organisations in:

- specifying a common privacy terminology;
- defining the actors and their responsibilities in processing PII;
- describing privacy safeguarding requirements; and
- referencing known privacy principles.

In terms of privacy protection controls, ISO 29100 uses quite general terminology, and it can be considered a basis for the detailed requirements and guidance in ISO 27701.

Cross-reference between PCF and ISO

In the table below, the PCF topics have been indicatively mapped to the ISO standards mentioned above.

Tag (PCF)	Topic (PCF)	Related controls ISO 27001:2013	Related controls ISO 27701:2019	Related Principles ISO 29100:2011
PPO	Privacy Policy	A.5.1.1, A.5.1.2, A.18.1.3, A.18.1.4 Clause: 5.2	A.7.2.1, A.7.2.2, A.7.3.1, A.7.3.10, B.8.2.1, B.8.2.6	Purpose legitimacy and specification Openness, transparency and notice Accountability
RRE	Definition of roles and responsibilities	A.6.1.1, A.7.1.2, A.7.2.1, A.15.1.1, A.15.1.2, A.15.1.3	5.2.1 A.7.2.7, B.8.2.1, B.8.2.6	Accountability

Tag (PCF)	Topic (PCF)	Related controls ISO 27001:2013	Related controls ISO 27701:2019	Related Principles ISO 29100:2011
		Clause: 5.1, 5.3		
PDI	Personal Data Identification and classification	A.8.1.1, A.8.2.1, A.8.2.2, A.8.2.3	A.7.2.1, A.7.2.2, A.7.2.8, A.7.3.10, B.8.2.2	Purpose legitimacy and specification
RMA	Risk Management	A.5.1.2 Clause: 6.1.1, 6.1.2, 6.1.3, 8.2	5.4.1.2	Accountability
PIA	Data Protection Impact Assessments	A.5.1.2, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.5 Clause: 6.1.2, 6.1.3, 8.2	5.4.1.2 A.7.2.5	Accountability
PIB	Privacy Incident and Breach Management	A.16.1.1 through A.16.1.7		Accountability
SCO	Staff competences	Clause: 7.2		Accountability
SAT	Staff awareness and training	A.7.2.2 Clause: 7.3		Accountability
LRC	Legal review of changes in regulatory and/or business requirements	A.18.1.1 Clause: 4.2		Privacy compliance
PST	Privacy statement	–	A.7.3.1, A.7.3.2, A.7.3.3	Openness, transparency and notice
CFR	Consent framework	–	A.7.2.3, A.7.2.4, A.7.3.4	Consent and choice
DMI	Data Minimisation	–	A.7.4.1, A.7.4.2, A.7.4.4	Data minimisation / Collection limitation

Tag (PCF)	Topic (PCF)	Related controls ISO 27001:2013	Related controls ISO 27701:2019	Related Principles ISO 29100:2011
ULI	Purpose limitation	–	A.7.4.1, A.7.4.2	Purpose legitimacy and specification
PBD	Privacy architecture (Privacy by Design and Privacy by Default)	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.5	A.7.4	Use, retention and disclosure limitation
DRE	Data retention	–	A..7.4.7	Use, retention and disclosure limitation
DDA	Disposal, destruction and anonymisation	A.8.3.1, A.8.3.2, A.11.2.7	A.7.4.5, A.7.4.8	Use, retention and disclosure limitation
URE	Use and restriction	–	A.7.3.5	Use, retention and disclosure limitation
DAR	Data access requests	–	A.7.3.3, A.7.3.6, A.7.3.7, A.7.3.8, A.7.3.9	Individual participation and access
DCR	Data correction requests	–	A.7.3.6, A.7.3.7, A.7.3.9	Individual participation and access / Accuracy and quality
DDR	Data deletion requests	A.8.3.1, A.8.3.2, A.11.2.7	A.7.3.6, A.7.3.7, A.7.3.9, B.8.4.2	Individual participation and access
DPR	Data portability requests	A.8.3.3	A.7.3.9	Individual participation and access
ACD	Accuracy and completeness of data	–	A.7.4.3	Accuracy and quality

Tag (PCF)	Topic (PCF)	Related controls ISO 27001:2013	Related controls ISO 27701:2019	Related Principles ISO 29100:2011
TPD	Third party disclosure and registration	A.8.3.3	A.7.5.1, A.7.5.3, A.7.5.4	Use limitation
TPA	Third party agreements	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	A.7.2.6, B.8.2.5, B.8.3.1, B.8.5.6, B.8.5.7, B.8.5.8	Accountability
DTR	Data Transfers	-	A.7.5.1, A.7.5.2, A.7.5.3, B.8.5.1, B.8.5.2	Accountability
ISP	Information Security Program	A.5.1.1, A.8.3.2, A.10.1.1, A.18.2.2, A.18.2.3		Information security
IAM	Identity and access management	A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2		Information security
STR	Secure transmission	A.10.1.1, A.13.1.1, A.13.1.2, A.13.1.3	A.7.4.9, B.8.4.3	Information security
ENC	Encryption and end-point security	A.8.1.4, A.8.3.1, A.8.3.2, A.10.1.1		Information security
LOG	Logging of access	A.12.4.1		Information security
REV	Review of privacy compliance	Clause: 9, 10 A.18.1.1, A.18.1.4		Privacy compliance
MON	Periodic monitoring on privacy controls	Clause 9, 10 A.18.2.1, A.18.2.2, A.18.2.3		Privacy compliance

For reasons of completeness, the following table provides an illustrative mapping of PCF subjects on ISO 27001 elements.

Cross-reference between ISO 27001, ISO 27002 and PCF topics		
ISO 27001:2013	**Subject**	**PCF**
Clause 4	Context of the organisation	LRC
Clause 5	Leadership	PPO, DDR
Clause 6	Planning	RMA
Clause 7	Support	SCO
Clause 8	Operation	RMA, PIA
Clause 9	Performance evaluation	REV, MON
Clause 10	Imporvement	REV, MON
A.5	Information security policies	PPO, RMA, PIA, ISP
A.6	Organization of information security	RRE, PIA, PBD
A.7	Human resource security	RRE, SAT
A.8	Asset management	PDI, DDA, DDR, DPR, TPD, ISP, ENC
A.9	Access control	IAM
A.10	Cryptography	ISP, STR, ENC
A.11	Physical and environmental security	DDA, DDR
A.12	Operations security	LOG
A.13	Communications security	STR
A.14	System acquisition, development & maintenance	PIA, PBD
A.15	Supplier relationships	RRE, TPA
A.16	Information security incident management	PIB
A.17	Information security aspects of BCM	
A.18	Compliance	PPO, LRC, ISP, REV, MON

ISO 27701:2019	**Subject**	**PCF**
A.7.2	Conditions for collection and processing	PPO, PDI, CFR, PIA, TPA, RRE,
A.7.3	Obligations to PII principals	PPO, PDI, PST, CFR, URE, DAR, DCR, DDR, DPR,
A.7.4	Privacy by design and default	DMI, ULI, ACD, DDA, DRE, STR
A.7.5	PII Sharing, transfer and disclosure	TPD, DTR
B.8.2	Conditions for collecting and processing	PPO, RRE, PDI, TPA
B.8.3	Obligations to PII principals	TPA
B.8.4	Privacy by design and default	DDR, STR
B.8.5	PII Sharing, transfer and disclosure	DTR, TPA