


NOREA Guide

Privacy Control Framework



Control objectives and controls
for privacy audits and
privacy assurance engagements

May 2018

Acknowledgement

This guide (in Dutch “Handreiking”) is issued by NOREA, the professional association of IT-auditors in the Netherlands and was developed for Dutch chartered IT-auditors (Register IT auditors, RE’s) to guide them to issue privacy control reports under the EU-General Data Protection Regulation (GDPR) and the International Standards on Assurance Engagements (ISAE). This Privacy Control Framework (PCF) provides the suitable criteria.

The PCF was built by a working group of NOREA between November 2017 and April 2018. The initial efforts were further elaborated and structured into this document, which was peer-reviewed and subsequently submitted for approval to NOREA’s Professional Practices Committee (“Vaktechnische Commissie”) on March 27th 2018.

Working group participants

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

drs. Jaap Boukens RE RA, Jeroen Caron RE MSc CIPP/E, ir. Jan de Heer RE, Maurice Koetsier RE MSc, 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

Coordination and editing

ir. Jan de Heer RE, Ed Ridderbeekx RE CISA CIPP/E

©2018 NOREA, All rights reserved
PO box 7984, 1008 AD Amsterdam
phone: +3120-3010380
e-mail: norea@norea.nl
www.norea.nl

Version control		
Version	Date	Amendments
0.91	March 2018	Review NOREA Professional Practices Committee
0.93	April 2018	Life Cycle Model adjusted
0.94	April 2018	Comments Professional Practices Committee processed
1.0	May 2018	Assurance section adjusted

Table of contents

Section 1 – Introduction	4
1. Introduction	5
2. Objectives of the Privacy Control Framework	5
3. Structure of the Privacy Control Framework	5
4. Privacy Control Framework and the GDPR	6
5. Use of the Privacy Control Framework	6
6. Disclaimer	7
7. How the Privacy Control Framework was established	7
Section 2. Privacy Control Framework – Overview	8
Section 3. Privacy Control Framework – Controls	14
Management	16
Notice	26
Choice and Consent	27
Collect	29
Use, store and dispose	30
Data access and data quality	35
Disclose	40
Data Security	43
Monitoring and Enforcement	48
Annex 1. Cross references PCF – GDPR	50
Cross reference of GDPR key elements with GDPR articles	51
Cross reference of GDPR articles with PCF's control objectives	52
Annex 2. Information Lifecycle	65
1. Introduction	66
2. Different Phases	67
3. Preconditions – management and stakeholders	68

Section 1 – Introduction

1. Introduction

This document presents the Privacy Control Framework of NOREA (Dutch Association of chartered IT-auditors / Nederlandse Orde van Register EDP-auditors), henceforth in this document referred to 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’, also see subsection 5 below).

In addition, the PCF can be deployed by an entity to assess the adequacy of privacy controls or to determine the gaps between the current state of privacy control and their ambitions in the light of (changing) legislative frameworks (e.g. the GDPR).

3. Structure of the Privacy Control Framework

The PCF prescribed control objectives has been defined e.g. making usage of the following ‘best practice’ frameworks (as stated by Koetsier and Ougajou in their thesis and subsequent [publication in “De IT-auditor”](#)):

- 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

The PCF is further structured along an information lifecycle management model (see also the [publication in “De IT-auditor”](#)). 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). Every privacy topic is linked to a control objective to be achieved, which subsequently has been operationalised by a number of

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

controls to be evaluated (104 in total). 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 thirteen (13) GDPR key elements. This was done based on professional opinion and e.g. the topics addressed in the document ‘In 10 stappen voorbereid op de AVG’ by the Autoriteit Persoonsgegevens. 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.

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 related 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 Article 29 Working Party) 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 aim to assess privacy maturity or GDPR-readiness;
- b. An IT-auditor who performs a privacy assurance engagement based on standard 3000 (‘NOREA Richtlijn 3000’) (either attestation (A) or direct reporting (D));
- c. Other professionals (such as risk managers, data protection-, security-, and privacy officers) who aim to assess privacy maturity or GDPR-readiness (non-audit) in an entity.

Privacy control assessment

For privacy control assessments, the practitioner involved can use the PCF as a general framework to be tailored 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 practitioner can determine which controls from section 3 should be evaluated. It is at the auditor's discretion to modify or enhance the controls to optimally fit the engagement scope and purpose.

Please note that the PCF does not make an explicit distinction between privacy control objectives to be achieved by *controllers* and those to be achieved by *processors*. The fact that (the part of) an entity under assessment can be clearly characterised as – for example– a processor only, might be a viable reason to exclude some of the controls in section 3 from the scope of work.

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').

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. As regards the controls from section 3, the 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, but 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 the IT-auditor to obtain sufficient and appropriate assurance evidence for a reasonable assurance conclusion.

6. Disclaimer

The PCF is intended to assist auditors and entities in assessing a privacy control framework. Any results, scoring or recommendations produced on the basis of applying the PCF should not be relied upon in isolation to determine how GDPR applies to an entity or an entity's compliance with GDPR, and the PCF does not constitute legal advice, certifications or guarantees regarding GDPR compliance. The application of GDPR is highly fact-specific and more practical implementation guidelines will be developed and published by regulatory and legislative bodies over time. We encourage all entities using the PCF to also work with a legally qualified professional to discuss GDPR, how it applies specifically to their organisation, and how best to ensure compliance.

7. 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 this document, which was peer-reviewed and subsequently submitted for approval to NOREA's Professional Practices Committee ("Vaktechnische Commissie") on March 27th 2018.

Section 2. Privacy Control Framework – Overview

The table below summarises the Privacy Control Framework. It contains 104 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 has established and communicated a policy that states its objectives and responsibilities regarding privacy and is in line with accepted privacy principles and applicable laws and regulations.	5
	DRR	Definition of roles and responsibilities	The entity has established and implemented clear roles and responsibilities regarding the safeguarding of personal data and the achievement of privacy objectives.	5
	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.	5
	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.	6
	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.	9

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	Use 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	3

Lifecycle phase	Tag	Topic	Control objective	# Controls
		and Privacy by Default)	regulations when designing or changing products, services, business systems or processes .	
	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.	3
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.	4
	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.	4
	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.	4
	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.	4
	ACD	Accuracy and completeness of data	Documented procedures for validation, editing and update of personal data assure accurate and complete personal data processing and the ability to access it when needed.	2

Lifecycle phase	Tag	Topic	Control objective	# Controls
enforcement		compliance	applicable privacy laws and regulatory requirements and decreases the risk of data breaches or loss of personal data.	
	MON	Periodic monitoring on privacy controls	The entity systematically and periodically assesses privacy processes and controls, as to establish that they operate as designed, resulting in ongoing compliance with applicable laws and regulatory requirements.	3

Section 3. Privacy Control Framework – Controls

Management	16
Notice	26
Choice and Consent	27
Collect	29
Use, store and dispose	30
Data access and data quality	35
Disclose	40
Data Security	43
Monitoring and Enforcement	48

Management

Privacy Policy (PPO)

Control objective:

The entity has established and communicated 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:

Evidence/testing:

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.	
PPO02	Management expresses its (responsibility for) commitment to solid and lawful privacy principles.	
PPO03	The privacy policy states the objectives of the entity regarding privacy and personal data protection.	
PPO04	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.	
PPO05	The entity has established and documented the criteria that ensure and demonstrate lawful processing for each instance of personal data processing.	

Related GDPR key elements:

- Privacy principles
- Lawfulness of processing
- Records of processing activities

Definition of roles and responsibilities (RRE)

Control objective:

The entity has established and implemented clear roles and responsibilities regarding the safeguarding of personal data and the achievement of privacy objectives.

Information Lifecycle Management phase: Management

Controls:

Evidence/testing:

RRE01	For every instance of processing personal data, the entity has established and documented whether it operates as controller or processor.	
RRE02	Where the entity operates as a processor, agreements with controllers are in place that govern the privacy responsibilities of the processor.	
RRE03	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.	
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.	
RRE05	The roles and responsibilities of individual staff in safeguarding personal data and compliance with privacy principles have been established and communicated.	

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:

Evidence/testing:

PDI01

The entity deploys a managed and 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.

PDI02

The entity clearly distinguishes and documents processing instances of (a) personal data and (b) special categories of personal data.

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.

PDI04

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).

Related GDPR key elements:

- Records of processing activities
- Privacy principles
- Security of processing

Risk Management (RMA)		
<i>Control objective:</i>		
The entity systematically and periodically identifies, assesses, and mitigates factors that endanger the achievement of privacy objectives.		
<i>Information Lifecycle Management phase: Management</i>		
<i>Controls:</i>		<i>Evidence/testing:</i>
RMA01	A process is in place to periodically identify the events endangering privacy objectives.	
RMA02	A process is in place to periodically assess the impact and probability of these events, and to subsequently formulate adequate risk responses and control measures.	
RMA03	When new or changed privacy risks are identified, the privacy risk assessment and the risk response strategies are reviewed and updated where needed.	
RMA04	Privacy risk acceptance criteria are approved, documented, and applied.	
RMA05	The entity plans and implements the controls that are necessary to mitigate privacy risk. Progress of implementation is monitored and measured.	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> • 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

<i>Controls:</i>		<i>Evidence/testing:</i>
PIA01	The entity deploys a managed and documented process to carry out an assessment of the impact on privacy regarding new or significantly changed processes, products and services.	
PIA02	The assessment takes into account the risks to data subject privacy presented by the changes envisaged, and the measures to mitigate these risks.	
PIA03	The assessment takes into account the purposes of processing in relation to the necessity and proportionality of processing personal data.	
PIA04	The process ensures that all relevant stakeholders are involved in the assessment, and that specific guidelines of the supervisory authority regarding assessment criteria are adhered to.	
PIA05	The entity documents all systems and software that process personal data and a history of changes applied to them.	
PIA06	The entity's change management process assures that approved privacy measures from the assessment have been implemented before the change is executed.	

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

<i>Controls:</i>		<i>Evidence/testing:</i>
PIB01	<p>A formal, comprehensive privacy incident and breach management process has been implemented, which specifies the following:</p> <ul style="list-style-type: none">a. The responsibilities of staff members to inform the responsible privacy officer in case of a privacy incident or possible data breach;b. The privacy officer (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 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).d. The privacy officer monitors the progress of remediating actions and reports to management (and, if applicable, informs the controller).	
PIB02	<p>The privacy officer has been assigned the overall responsibility for the breach management process.</p> <p>Incidents and breaches that do not involve personal data are the responsibility of the security officer.</p>	
PIB03	<p>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.</p>	
PIB04	<p>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.</p>	
PIB05	<p>The process ensures that all required information regarding the breach is collected and provided to the supervisory authority, including mitigating measures.</p>	

PIB06	The privacy officer has been assigned the overall responsibility for the breach notification process. The privacy documents all considerations made when determining the obligation to notify.	
PIB07	The breach management process outlines that lessons learned from breaches lead to remediations and improvements, and serve as input for staff privacy awareness programs.	
PIB08	<p>The privacy incident and breach management process also specifies the following:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> o incident root cause; o incident patterns; o changes in the internal control environment and legislation; o results of the periodic review and progress of improvements are reported to and reviewed by management. 	
PIB09	The breach management process is reviewed at least every year and shortly after the implementation of significant system or procedural changes.	
<p><i>Related GDPR key elements:</i></p> <ul style="list-style-type: none"> • Personal Data Breach 		

Staff competences (SCO)		
<i>Control objective:</i>		
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.		
<i>Information Lifecycle Management phase: Management</i>		
<i>Controls:</i>		<i>Evidence/testing:</i>
SCO01	The entity has documented and formalised the required privacy competences for staff that is involved in handling personal data. It also has established how these competences can be achieved (e.g. training programs).	
SCO02	The entity documents the extent to which individual staff members possess these competences. A process is in place to bridge competence gaps.	
SCO03	The entity addresses privacy competences in its hiring and onboarding process, and addresses privacy performance in individual appraisals.	
SCO04	Management annually reviews the allocation of staff, budgets, and other resources to its privacy program.	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> • 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

<i>Controls:</i>		<i>Evidence/testing:</i>
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.	
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.	
SAT03	Training and awareness courses are reviewed and updated to reflect current legislative, regulatory, industry, and entity policy and procedure requirements.	

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:

Evidence/testing:

LRC01	<p>The entity deploys a process to monitor, assess, and address the impact on privacy requirements from changes in:</p> <ol style="list-style-type: none">legal and regulatory requirements;industry requirements, best practices and guidelines;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);business operations and processes;people assigned responsibility for privacy and security matters;technology (prior to implementation).
--------------	---

Related GDPR key elements:

- Data Protection Impact Assessment
- Lawfulness of processing

Notice

Privacy statement (PST)		
<p><i>Control objective:</i></p> <p>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.</p>		
<p><i>Information Lifecycle Management phase:</i> Notice</p>		
<i>Controls:</i>		<i>Evidence/testing:</i>
PST01	<p>The entity's privacy statement:</p> <ol style="list-style-type: none"> describes the personal data obtained, the sources of such information, the purposes for which it is collected and the applicable lawfulness criteria; describes the consequences, if any, of the data subject not providing the requested information; describes (if applicable) further processing. 	
PST02	<p>The privacy statement is:</p> <ol style="list-style-type: none"> easily accessible and (made) available for data subjects when personal data is first collected from the data subject; 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; 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. 	
<p><i>Related GDPR key elements:</i></p> <ul style="list-style-type: none"> • Rights of the data subject • Responsibilities of the controller / processor • Privacy principles 		

Choice and Consent

Consent framework (CFR)		
<i>Control objective:</i>		
The entity obtains data subject's consent for processing personal data where required or necessary.		
<i>Information Lifecycle Management phase: Choice and consent</i>		
<i>Controls:</i>		<i>Evidence/testing:</i>
CFR01	<p>The entity's privacy statement describes, in a clear and concise manner, the following:</p> <ul style="list-style-type: none"> a. the choices available to the individual regarding the collection, use, and disclosure of personal data; b. the process an individual 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). 	
CFR02	<p>If processing is based on data subject's consent, the entity:</p> <ul style="list-style-type: none"> 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. 	
CFR03	<p>The entity does not collect or process special categories of personal data, unless it has a lawful basis to do.</p> <p>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</p>	

	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.	
<p><i>Related GDPR key elements:</i></p> <ul style="list-style-type: none"> • 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:

Evidence/testing:

DMI01

A process and procedures are in place 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.

DMI02

The privacy policy states data minimisation as a privacy principle for the entity (see PPO).

Related GDPR key elements:

- Privacy principles
- Privacy By Design / by Default

Use, store and dispose

Use 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:

Evidence/testing:

ULI01

A process and procedures are in place 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.

ULI02

The privacy policy states use limitation as a privacy principle for the entity (see PPO).

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:

Evidence/testing:

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 third parties in these activities, it will require these third parties to deploy the same privacy risk management activities.

PBD02 Assessment of privacy risks is an inherent and documented element of the entity's project methodology and/or design and development process.

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.

Related GDPR key elements:

- Privacy by Design / by Default
- Privacy principles

Data retention (DRE)		
<i>Control objective:</i>		
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.		
<i>Information Lifecycle Management phase:</i> Use, store and dispose		
<i>Controls:</i>		<i>Evidence/testing:</i>
DRE01	<p>The entity:</p> <ol style="list-style-type: none"> documents its retention policies and disposal procedures for personal data; ensures personal data is not kept beyond the established retention time unless a justified business or legal reason for doing so exists; for each instance of personal data processing, documents applicable retention times; discloses retention time policies to data subjects in its privacy statement; retains, stores, and disposes archived and backup copies of records in accordance with its retention policies. 	
DRE02	Contractual requirements are considered when establishing retention practices when they may be exceptions to normal policies.	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> 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:

Evidence/testing:

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:

within the limits of technology, locates and removes or reduces specified personal data about an individual as required, for example, removing credit card numbers after the transaction is complete;
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.

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.

Related GDPR key elements:

- Privacy principles
- Responsibilities of the controller / processor
- Security of processing
- Privacy By Design / by Default

Use and restriction (URE)		
<i>Control objective:</i>		
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.		
<i>Information Lifecycle Management phase: Use, store and dispose</i>		
<i>Controls:</i>		<i>Evidence/testing:</i>
URE01	The entity communicates to the data subject the steps to be taken to exercise the right to restriction of processing and the right to object to processing, and the valid criteria to do so.	
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.	
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.	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> • 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)		
<i>Control objective:</i>		
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.		
<i>Information Lifecycle Management phase: Data access and data quality</i>		
<i>Controls:</i>		<i>Evidence/testing:</i>
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).	
DAR02	The entity informs the data subject of the existence of this right and the procedure to exercise this right in the privacy statement.	
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.	
DAR04	The entity verifies the identity of the requesting data subject before responding.	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> • 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:

Evidence/testing:

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.	
DCR02	The entity informs the data subject of the existence of this right and the procedure to exercise it in the privacy statement.	
DCR03	The entity verifies the identity of the requesting data subject before acting on the request.	
DCR04	The entity notifies third parties, to whom personal data has been disclosed, of necessary corrections in personal data.	

Related GDPR key elements:

- Rights of the data subject

Data deletion requests (DDR)		
<i>Control objective:</i>		
Data deletion requests are responded to adequately and data subjects are able to have their personal data deleted if applicable criteria are met.		
<i>Information Lifecycle Management phase:</i> Data Access and data quality		
<i>Controls:</i>		<i>Evidence/testing:</i>
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.	
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.	
DDR03	The entity informs the data subject of the existence of this right and the procedure to exercise this right in the privacy statement.	
DDR04	The entity verifies the identity of the requesting data subject before acting on the request.	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> • Rights of the data subject 		

Data portability requests (DPR)		
<i>Control objective:</i>		
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.		
<i>Information Lifecycle Management phase: Data Access and data quality</i>		
<i>Controls:</i>		<i>Evidence/testing:</i>
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.	
DPR02	If technically feasible, the entity will transfer the personal data directly to another (controlling) entity as instructed by the data subject.	
DPR03	The entity informs the data subject of the existence of this right and the procedure to exercise this right in the privacy statement.	
DPR04	The entity verifies the identity of the requesting data subject before acting on the request.	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> • Rights of the data subject • Right to data portability 		

Accuracy and completeness of data (ACD)		
<i>Control objective:</i>		
Documented procedures for validation, editing and update of personal data ensure accurate and complete personal data processing and the ability to access it when needed.		
<i>Information Lifecycle Management phase:</i> Data Access and data quality		
<i>Controls:</i>		<i>Evidence/testing:</i>
ACD01	<p>The entity has procedures in place to:</p> <ol style="list-style-type: none"> edit and validate personal data as it is collected, created, maintained, and updated; record the date when the personal data is obtained or updated; specify when the personal data is no longer valid; 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); 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; ensure personal data processed is sufficiently accurate and complete to make decisions. 	
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.	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> Security of processing 		

Disclose

Third party disclosure and registration (TPD)

Control objective:

Personal data is not disclosed to third parties, or further processed for purposes for which the individual has not consented to.

Information Lifecycle Management phase: Disclose

Controls:

Evidence/testing:

TPD01

The entity has procedures in place to:

- a. prevent the disclosure of personal data to third parties unless the data subject has given consent for the disclosure;
- b. document the nature and extent of personal data disclosed to third parties;
- c. 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;
- d. document any third-party disclosures for legal reasons;
- e. notify individuals and obtain their consent prior to disclosing personal data to a third party for purposes not identified in the privacy notice;
- f. monitor that personal data is only provided to third parties for purposes specified in the privacy notice.

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:

Evidence/testing:

TPA01	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.	
TPA02	The entity ensures that the agreements will also address the following obligations of the third party: <ul style="list-style-type: none">a. confidentiality and non-disclosure;b. security requirements;c. cooperation in responding to data subject requests and data subject rights execution;d. information provision (e.g. in case of planned subcontracting);e. information provision and cooperation in case of data breaches;f. retention periods and data deletion;g. no further subcontracting without permission of the entity;h. liabilities and indemnifications.	
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): <ul style="list-style-type: none">a. the third party responds to a questionnaire about its practices; the third party self-certifies that its practices meet the entity's requirements based on internal audit reports or other procedures; the entity performs a periodic on-site evaluation of the third party; 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.

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.

Related GDPR key elements:

- Transfers of personal data to third countries or international organisations

Data Security

Information Security Program (ISP)		
<i>Control objective:</i>		
Personal data is adequately secured from accidental errors or loss, or from malicious acts such as hacking or deliberate theft, disclosure or loss.		
<i>Information Lifecycle Management phase: Data security</i>		
<i>Controls:</i>		<i>Evidence/testing:</i>
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.	
ISP02	Security of personal data is explicitly addressed in the entity's information security policies and the information security management system.	
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.	
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).	
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.	
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.	
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).	
<i>Related GDPR key elements:</i>		
<ul style="list-style-type: none"> • Security of processing 		

Identity and access management (IAM)

Control objective:

Assignment of appropriate access rights, appropriate changes to access rights and timely removal of access rights decreases 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:

Evidence/testing:

IAM01	<p>Systems and procedures are in place to:</p> <ol style="list-style-type: none">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;authenticate users, for example, by user name and password, certificate, external token, or biometrics before access is granted to systems handling personal data;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;implement intrusion detection and monitoring systems.
-------	--

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:

Evidence/testing:

STR01

Systems and procedures are in place to:

- a. define minimum levels of encryption and controls;
- 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.

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:

Evidence/testing:

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.

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.

ENC03 Procedures exist for creation, transfer, storage, and disposal of media containing personal data used for backup and recovery.

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.

Related GDPR key elements:

- Security of processing
- Personal Data Breach

Logging of access (LOG)

Control objective:

The entity detects and investigates access or access attempts to personal data by staff, third parties or hackers that could result in a breach, sabotage of systems, insertion of malicious code, theft of personal data, etc.

Information Lifecycle Management phase: Data security

Controls:

Evidence/testing:

LOG01	Systems and procedures are in place to: <ul style="list-style-type: none">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.	
--------------	---	--

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:

Evidence/testing:

REV01	<p>Systems and procedures are in place to:</p> <ol style="list-style-type: none">annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service level agreements, standards adopted by the entity, and other contracts;document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign-offs;report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan;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).
--------------	--

Related GDPR key elements:

- Lawfulness of processing

Periodic monitoring on privacy controls (MON)

Control objective:

The entity systematically and periodically assesses privacy processes and controls, as to establish that they operate as designed, resulting in ongoing compliance with applicable laws and regulatory requirements.

Information Lifecycle Management phase: Monitoring and enforcement

<i>Controls:</i>		<i>Evidence/testing:</i>
MON01	Management of the entity reviews the following to ensure operational effectiveness of privacy controls: <ul style="list-style-type: none">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.	
MON02	The selection of controls to be monitored, reviewed and/or audited and the frequency with which this is performed are based on the sensitivity of the personal data involved and the risks of possible exposure or loss.	
MON03	The entity deploys a process that ensures that monitoring leads to remediation of shortcomings and continuous improvement.	
<i>Related GDPR key elements:</i> <ul style="list-style-type: none">• 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 the GDPR key elements and the articles in the GDPR.

GDPR key element	GDPR article(s)
Privacy Principles	5
Lawfulness of Processing	6
Conditions for Consent	7
Rights of the data subject	12–19
Right to data portability	20
Privacy By Design / by Default	25
Responsibilities of controller and processor	24, 28
Records of processing activities	30
Security of processing	32
Personal Data Breach	33, 34
Data Protection Impact Assessment (DPIA)	35
Data Protection Officer (DPO)	37–39
Transfers of personal data to third countries or international organisations	44–50

Cross reference of GDPR articles with PCF's control objectives

GDPR key element: "Privacy Principles"	
GDPR article reference	Xref to Controls of Privacy Control Framework
<p>Article 5 Principles relating to processing of Personal data Article 5 will be stated fully below.</p> <p>1. Personal data shall be:</p> <ol style="list-style-type: none"> processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). <p>2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')</p>	<p>Privacy Policies (PPO)</p> <p>Definition of roles and responsibilities (RRE) – RRE05</p> <p>Staff competences (SCO)</p> <p>Personal Data Identification and classification (PDI)</p> <p>Staff awareness and training (SAT)</p> <p>Use limitation (ULI)</p> <p>Privacy statement (PST)</p> <p>Data Minimisation (DMI)</p> <p>Use limitation (ULI)</p> <p>Privacy architecture (Privacy by Design and Privacy by Default)</p> <p>Data retention (DRE)</p> <p>Disposal, destruction and anonymisation (DDA)</p> <p>Use and restriction (URE)</p>

GDPR key element: “Lawfulness of Processing” and “Conditions for Consent”	
<i>GDPR article reference</i>	<i>Xref to Controls of Privacy Control Framework</i>
<p>Article 6 Lawfulness of processing</p> <p><u>Summary:</u> Lawful processing must:</p> <ul style="list-style-type: none"> a. be consented to by the subject for the stated purpose; b. be required by a contract; c. be necessary for other compliance reasons (legal obligations); d. be necessary to protect someone’s vital interests; e. be required for public interest or an official authority; f. be limited if the subject is a child. <p>Article 7 Conditions for consent</p> <p><u>Summary:</u> The data subject’s consent must be informed, freely given. The data subject shall have the right to withdraw his or her consent at any time and they can withdraw it easily at any time.</p>	<p>Privacy Policy (PPO)</p> <p>Consent framework (CFR)</p> <p>Legal review of changes in regulatory and/or business requirements (LRC)</p> <p>Use and restriction (URE)</p> <p>Third party disclosure and registration (TPD)</p> <p>Review of privacy compliance (REV)</p> <p>Periodic monitoring on privacy controls (MON)</p>

GDPR key element: "Rights of the data subject"	
<i>GDPR article reference</i>	<i>Xref to Controls of Privacy Control Framework</i>
<p><u>Summary:</u></p> <p>The list of information that needs to be given to data subjects is expanded under the GDPR – see the different related articles.</p> <p>Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject</p> <p>Article 13 – Information to be provided where personal data are collected from the data subject</p> <p>Article 14 – Information to be provided where personal data have not been obtained from the data subject</p> <p>Article 15 – Right of access by the data subject</p> <p>Article 16 – Right to rectification</p> <p>Article 17 – Right to erasure ('right to be forgotten')</p> <p>Article 18 – Right to restriction of processing</p> <p>Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing</p> <p>Article 20 – Right to data portability – see next section (table)</p>	<p>Use and restriction (URE)</p> <p>Data access requests (DAR)</p> <p>Consent framework (CFR)</p> <p>Privacy statement (PST)</p> <p>Data correction requests (DCR)</p> <p>Data deletion requests (DDR)</p>

GDPR key element: : “Right to data portability”	
<i>GDPR article reference</i>	<i>Xref to Controls of Privacy Control Framework</i>
<p>Article 20 Right to data portability</p> <p><u>Summary:</u> Article 20.1</p> <p>The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.</p> <p>In other words: people have the right to obtain a usable ‘portable’ electronic copy of their personal data to pass to a different controller.</p>	Data portability requests (DPR)

GDPR key element: “ Responsibilities of “Controller” and Processor” “	
GDPR article reference	Xref to Controls of Privacy Control Framework
<p>Article 24 Responsibility of the controller</p> <p><u>Summary:</u></p> <p>A controllers determines the “purpose and the means” of the use of personal data.</p> <p>Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures.</p> <p>The controller must be able to demonstrate that processing is performed in accordance with this Regulation (“Accountability”).</p> <p>Those measures shall be reviewed and updated where necessary.</p> <p>If the controller wishes to hire a processor, the controller must select a party “providing sufficient guarantees to implement appropriate technical and organizational measures” to ensure the protection of the rights of the data subject.</p> <p>If appropriate the controller must sign a contract with the processor setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller, including the appropriate security measures.</p> <p>Article 28 Processor</p> <p><u>Summary:</u></p> <p>A processors processes the personal data “on behalf of the controller”.</p> <p>The processor must provide sufficient guarantees to implement appropriate technical and organizational measures to ensure the protection of the rights of the data subject.</p> <p>Any (external) party that has access to personal data and is engaged by the controller is regarded as a “processor”.</p> <p>The processor cannot outsource the processing to a sub-processor without the written consent of the controller.</p>	<p>Definition of roles and responsibilities (RRE)</p> <p>Privacy statement (PST)</p> <p>Data retention (DRE)</p> <p>Disposal, destruction and anonymisation (DDA)</p> <p>Third party agreements (TPA)</p>

GDPR key element: "Privacy By Design / by Default"

GDPR article reference	Xref to Controls of Privacy Control Framework
<p>Article 25 Data protection by design and by default</p> <p>Articles 25.1 and 25.2 are stated below:</p> <ol style="list-style-type: none"> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to <i>implement data-protection principles, such as data minimisation</i>, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. <p>NOTE relation exists with article 35 Data Protection Impact Assessment for defining the appropriate mitigating measures.</p> <ol style="list-style-type: none"> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by <i>default</i>, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 	<p>Risk Management (RMA)</p> <p>Definition of roles and responsibilities (RRE)</p> <p>Staff competences (SCO)</p> <p>Data Minimisation (DMI)</p> <p>Use limitation (ULI)</p> <p>Privacy architecture (Privacy by Design and Privacy by Default) (PBD)</p> <p>Data access requests (DAR)</p> <p>Disposal, destruction and anonymisation (DDA)</p>

GDPR key element: "Records of processing activities"	
GDPR article reference	Xref to Controls of Privacy Control Framework
<p>Article 30 Records of processing activities</p> <p><u>Summary:</u></p> <p>Article 30.1 Each controller and, where applicable, the controller's representative, shall maintain a record (in writing or electronic form) of processing activities. This record contains the following elements:</p> <ol style="list-style-type: none"> 1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; 2. the purposes of the processing; 3. a description of the categories of data subjects and of the categories of personal data; 4. where applicable, transfers of personal data to a third country or an international organization; 5. time limits for erasure of the different categories of data; 6. a general description of the technical and organisational security measures (see article 32). <p>Article 30.2 Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller. See article 30.1.</p> <p>Article 30.4 The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.</p>	<p>Privacy Policy (PPO)</p> <p>Definition of roles and responsibilities (RRE)</p> <p>Personal Data Identification and classification (PDI)</p>

GDPR key element: "Security of Processing"	
<i>GDPR article reference</i>	<i>Xref to Controls of Privacy Control Framework</i>
<p>Article 32 Security of Processing</p> <p><u>Summary:</u></p> <p>The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk; examples of measures:</p> <ol style="list-style-type: none"> 1. the pseudonymisation and encryption of personal data; 2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 3. the ability to restore timely the availability and access to personal data in the event of a physical or technical incident; 4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures. <p><u>Guidance:</u></p> <p>An ISO27k related Quality System – ISMS provides a coherent, comprehensive and structured framework to manage privacy alongside other information risk and security controls, compliance etc.</p>	<p>Personal Data Identification and classification (PDI)</p> <p>Staff competences (SCO)</p> <p>Staff awareness and training (SAT)</p> <p>Definition of roles and responsibilities (RRE)</p> <p>Disposal, destruction and anonymisation (DDA)</p> <p>Data access requests (DAR)</p> <p>Accuracy and completeness of data (ACD)</p> <p>Third party disclosure and registration (TPD)</p> <p>Third party agreements (TPA)</p> <p>Information Security Program (ISP)</p> <p>Identity and access management (IAM)</p> <p>Secure transmission (STR)</p> <p>Encryption and end-point security (ENC)</p> <p>Logging of access (LOG)</p>

GDPR key element: "Personal Data Breach"	
<i>GDPR article reference</i>	<i>Xref to Controls of Privacy Control Framework</i>
<p>Article 33 Notification of a personal data breach to the supervisory authority</p> <p><u>Summary:</u></p> <p>In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. Notification is not necessary when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.</p> <p>The processor shall notify the controller without undue delay after becoming aware of a personal data breach.</p> <p>The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.</p> <p>Article 34 Communication of a personal data breach to the data subject</p> <p><u>Summary:</u></p> <p>Art. 34.1: When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.</p> <p>The communication to the data subject referred to the above mentioned article shall not be required if i.e. the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.</p>	<p>Privacy Incident an Breach Management (PIB)</p> <p>Secure transmission (STR)</p> <p>Encryption and end-point security (ENC)</p> <p>Logging of access (LOG)</p>

GDPR key element: Data Protection Impact Assessment (DPIA)"	
GDPR article reference	Xref to Controls of Privacy Control Framework
<p>Article 35 Data Protection Impact Assessment</p> <p>Articles 35.1, 35.2, 35.3 and article 35.7 are stated below:</p> <ol style="list-style-type: none"> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: <ol style="list-style-type: none"> a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or a systematic monitoring of a publicly accessible area on a large scale. <p><i>Relevant for the output of the DPIA is article 7:</i></p> <ol style="list-style-type: none"> The assessment shall contain at least: <ol style="list-style-type: none"> a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. 	<p>Risk Management (RMA)</p> <p>Data Protection Impact Assessments (PIA)</p> <p>Legal review of changes in regulatory and/or business requirements (LRC)</p>

Guidance related to DPIA:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171013_wp248_rev01_enpdf.pdf

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia>

GDPR key element: "Data Protection Officer (DPO)"	
GDPR article reference	Xref to Controls of Privacy Control Framework
<p>Article 37 Designation of the data protection officer</p> <p><u>Summary:</u></p> <p>The GDPR provides that a controller or processor must designate a data protection officer when: (i) the processing is carried out by a public authority; (ii) it regularly and systematically monitors data subjects on a large scale; or (iii) processes sensitive personal data on a large scale.</p> <p>A group of companies may appoint a single data protection officer if the latter is easily accessible from each establishment within the group.</p> <p>Article 38 Position of the data protection officer</p> <p><u>Summary:</u></p> <p>The GDPR also sets out a profile description of the DPO: he or she must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. The DPO may be a staff member or external consultant and may have other (internal or external) tasks in addition to the role of DPO.</p> <p>The DPO must ensure compliance within the company and therefore may need to defend the interests of data subjects against the (economic) interests of the company. Therefore, the DPO must be independent in the company's organization, and must report to the highest level of management. The DPO is also protected against dismissal or other sanctions for performing his or her tasks.</p> <p>Article 39 Tasks of the data protection officer</p> <p><u>Summary:</u></p> <p>The data protection officer's key tasks include: (i) informing and advising the company on data protection compliance; (ii) advising as regards data protection impact assessments; (iii) monitoring compliance with relevant data protection provisions which includes, for instance, training of staff member and related audits; (iv) and cooperating and acting as a contact point for Data Protection Authorities (DPA)s.</p> <p>Guidance related to data protection officers:</p> <p>-https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg</p>	<p>Definition of roles and responsibilities (RRE)</p> <p>Staff competences (SCO)</p>

GDPR key element: "Transfers of personal data to third countries or international organisations"	
<i>GDPR article reference</i>	<i>Xref to Controls of Privacy Control Framework</i>
<p>Article 44 up to and including article 50</p> <p><u>Summary:</u></p> <p>To ensure that the protection granted by the GDPR is not undone when personal data is transferred, the GDPR, in principle, only permits personal data to be transferred to third countries which have been found to provide an adequate level of protection by the European Commission.</p> <p>Policies and procedures must be in place to manage international data transfers to other countries. Data transfers are allowed to countries that ensure an adequate level of protection. If a particular country does not guarantee an adequate level of protection, unambiguous consent, the necessity of the transfer for performance of a contract, a set of standard contractual clauses approved by the European Commission, or Binding Corporate Rules (BCR) are tolerated derogations (as listed in article 26 of Directive 95/46/EC).</p>	<p>Definition of roles and responsibilities (RRE)</p> <p>Use and restriction (URE)</p> <p>Data Transfers (DTR)</p>

Annex 2. Information Lifecycle

1. 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:

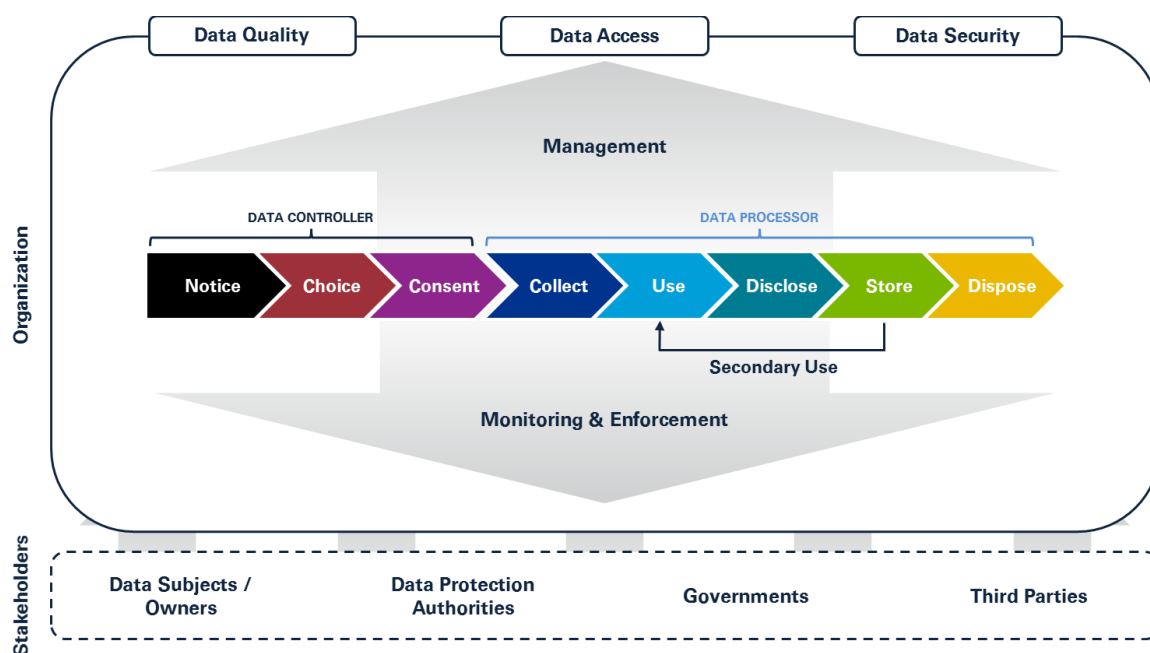


Figure 1 Information Lifecycle Model

2. Different Phases

The information life cycle model has been based and defined upon a mix of GAPP⁵-principles and OECD-⁶principles. 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.

The first three phases of the information lifecycle model (notice, choice and consent) are under the responsibility of the **Data Controller**. In these processes, personal data of data subjects is not (yet) processed. Processing of personal data is being prepared by the Data Controller: requirements are met before processing of personal data actually can take place.

⁵ GAPP, An Executive Overview of GAPP: Generally Accepted Privacy Principles, 2009.

⁶ The OECD Privacy Framework, Organisation for Economic Co-operation and Development, 2013.

The last five phases of the information lifecycle model (collect, use, disclose, store, and dispose) are grouped under the **Data Processor**: this is the organization that actually processes the personal data (this can also be the Data Controller). From the phase Collect, personal data of the data subject is used and this ends after the final phase Dispose has been completed.

3. 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 a Privacy Control Framework (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.

In this way a clear overview is present of the different privacy control objectives positioned in the phases of the information lifecycle model. We can conclude that making usage of this model the governance of personal data in entities can be significantly improved.