Naar een nieuw Privacy Control Framework (PCF)

Ed Ridderbeekx

22 november 2017

KENNISGROEP P R I V A C Y

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Een stukje geschiedenis

- 2001: Raamwerk Privacy Audit (door ‘Samenwerkingsverband Audit Aanpak’ onder verantwoordelijkheid CPB)
- 2002: ZekeRE Privacy (NOREA)
- 2006: Richtlijn 3600 Assurance–opdrachten met betrekking tot Persoonsgegevens (NBA, NOREA)
- 2006: Keurmerk ‘Privacy Audit Proof’(NBA, NOREA)
- 2016: Addendum NOREA Privacy Audit 2016 bij Richtlijn 3600n (NOREA)
- 2017: Besluit Bestuur i.o.m. KG Privacy en Vaktechnische Commissie om zowel Raamwerk als Richtlijn voor privacy audits te vernieuwen, mede in het licht van de AVG.

Een nieuw Privacy Control Framework

- Actualiteit en marktvraag:
- AVG
- Implementatie én auditing
- Accountability en aantoonbaarheid
- Onderscheidend vermogen

Opdracht en Uitgangspunten

- Vernieuw en actualiseer de geldende richtlijn voor assurance–opdrachten en het Raamwerk Privacy Audit zodat het aansluit bij ontwikkelingen in het veld, met name de AVG.
- Uitgangspunt (rapportageformat): kijk of inbedding in NOREA Handreiking voor Richtlijn (ISAE) 3000 / SOC rapporten voor IT Service Organisaties met Trust Service Principles & Criteria mogelijk is.
- Uitgangspunt (raamwerk): kijk of het mogelijk is gebruik te maken van een uitgekristalliseerd raamwerk voor privacy audits.

Hiermee is de (sub)werkgroep Privacy Control Framework in oktober 2017 aan de slag gegaan.

Het PCF van Koetsier, Ougajou en Nanninga

- ...ziet privacy als onderdeel van informatiemanagement (+)
- ...is gebaseerd op privacy principes en meerdere international normstelsels (+)
- ...is uitgewerkt en beschikbaar (+)

- ...maar hoe zit het met aansluiting met de AVG?

Control ID	Control name	Control domain	Link to information lifecycle model
1.1	Privacy Policies	Privacy Policies	Management
1.2	Privacy Roles & Responsibilities	Privacy Officer ('FG')	Management
1.3	Personal Data Identification and Classification	Data Infrastructure	Management
1.4	Risk Assessment	Risk and Control Framework	Management
1.5	Privacy Impact Assessment for New Products & Services, Processes and Systems	Privacy Processes	Management
1.6	Privacy Incident and Breach Management	Privacy Incident and Breach Management	Management
1.7	Qualifications of Internal Personnel	Training and Awareness	Management
1.8	Privacy Awareness and Training	Training and Awareness	Management
1.9	Legal Review of Changes in Regulatory and Business Requirements	Legal Processes	Management
2.1	Privacy Notice / Statement	Privacy Policies	Notice
2.2	Registration with the Data Protection Authorities	Privacy Processes	Notice
3.1	Consent Framework (opt-ins / opt-outs)	Information Lifecycle Management	Choice and Consent
4.1	Data Minimisation (Collection)	Information Lifecycle Management	Collect
5.1	Use Limitation of Personal Data	Information Lifecycle Management	Use, Store and Dispose
5.2	Privacy Architecture (Privacy by Design)	Privacy Architecture / Requirements	Use, Store and Dispose
5.3	Data Retention	Information Lifecycle Management	Use, Store and Dispose
5.4	Disposal, Destruction and Anonymization	Information Lifecycle Management	Use, Store and Dispose
6.1	Data Access Requests	Privacy Processes	Data Access
6.2	Data Correction Requests	Privacy Processes	Data Access & Data Quality
6.3	Data Deletion Requests	Privacy Processes	Data Access
7.1	Third Party Disclosure and Registration	Third Party Management	Disclose
7.2	Third Party Agreements	Third Party Management	Disclose
7.3	Data Transfers to non-EU and non-EEA countries	Privacy Processes	Disclose
8.1	Information Security Program	Information Security Management	Data Security
8.2	Identity & Access Management	Information Security Management	Data Security
8.3	Secure Transmission of Personal Data	Information Security Management	Data Security
8.4	Encryption of Personal Data on Portable Media	Information Security Management	Data Security
8.5	Logging of Access to (Sensitive) Personal Data	Information Security Management	Data Security
9.1	Accuracy and Completeness of Personal Data	Privacy Processes	Data Quality
10.1	Review on Privacy Compliancy	Accountability & Auditing	Monitoring and Enforcement
10.2	Periodic Monitoring on Privacy Controls	Accountability & Auditing	Monitoring and Enforcement

Mapping met artikelen uit AVG

Control ID	Control name	Control domain	Link to information lifecycle model	Reference to art. in GDPR
1.1	Privacy Policies	Privacy Policies	Management	(5, 6)
1.2	Privacy Roles & Responsibilities	Privacy Officer ('FG')	Management	5
1.3	Personal Data Identification and Classification	Data Infrastructure	Management	
1.4	Risk Assessment	Risk and Control Framework	Management	
1.5	Privacy Impact Assessment for New Products & Services, Processes and Systems	Privacy Processes	Management	
1.6	Privacy Incident and Breach Management	Privacy Incident and Breach Management	Management	
1.7	Qualifications of Internal Personnel	Training and Awareness	Management	
1.8	Privacy Awareness and Training	Training and Awareness	Management	
1.9	Legal Review of Changes in Regulatory and Business Requirements	Legal Processes	Management	
2.1	Privacy Notice / Statement	Privacy Policies	Notice	(5, 6)
2.2	Registration with the Data Protection Authorities	Privacy Processes	Notice	
3.1	Consent Framework (opt-ins / opt-outs)	Information Lifecycle Management	Choice and Consent	(7,8)
4.1	Data Minimisation (Collection)	Information Lifecycle Management	Collect	5

Mapping met artikelen uit AVG

Privacy Risk & Control Framework					
Control I	Phase from the information lifecycle model	Control Nam	Privacy risk	Management criteria	Mitigating measures
01.1	Management	Privacy Policies	Employees, business partners and third parties are unaware of the organisation's minimum requirements with regard to the collection, use, retention, disclosure and disposal of personal data.	The entity defines and documents its privacy policies with respect to the GAPP principles: a. Notice b. Choice and consent c. Collection d. Use, retention and disposal e. Access f. Disclosure to third parties g. Security for Privacy h. Quality i. Monitoring and Enforcement	Privacy policies are documented in writing and made readily available to internal personnel and third parties who need them. Privacy policies and procedures are: - reviewed and approved by senior management or a management committee. - reviewed at least annually and updated as needed.
01.1 a	Management	Privacy Policies	Processing of personal data is not in line with solid, accepted, and legally binding privacy principles	The entity ensures that processing of personal data is based on privacy principles: - lawfulness, fairness, transparancy - purpose limitation - data minimisation - accuracy - storage limitation - integrity and confidentiality	Management expresses its adherence to solid privacy principles as an explicit part of its privacy policy. 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.
01.1b	Management	Privacy Policies	Processing of personal data is unlawful	The entity only processes personal data if processeing is based on a lawful criterium.	For existing processing of personal data, the entity will establish and document the underlying criteria that ensure lawful processing. For new or plaaned processing, the entity systematically assesses the lawfulness criteria. Depending on the specific criteria, additionally required actions are planned and executed (eg. acquiring and documenting consent if 'consent' is the applicable criterium)

Aansluiting met AVG

- De aansluiting met kernelementen van de AVG is geborgd:
  - Privacy principes
  - Rechtmatigheidsgrondslag
  - Rechten van betrokkene
  - Privacy by Design / by Default
  - DPIA / gegegevensbeschermingseffectbeoordeling
  - Functionaris Gegevensbescherming
  - Verantwoordelijkheden VV en V
  - Transfers/international/BCRs

Hoe verder?

- Binnen enkele weken finaliseren we het PCF
- We monitoren nieuwe guidance (Article 29 WP, AP) en verwerken die waar nodig
- Het privacy–instrumentarium van de NOREA zal dan bestaan uit:
  - Handreiking Privacy Impact Asessments
  - Handreiking Werkprogramma Meldplicht Datalekken
  - Privacy Control Framework
  - Rapportageformat privacy audits conform Richtlijn 3000

Bedankt

Voor meer informatie kun je contact opnemen met:

Ed Ridderbeekx
06-12504784
ed@greendots.nl

22 november 2017