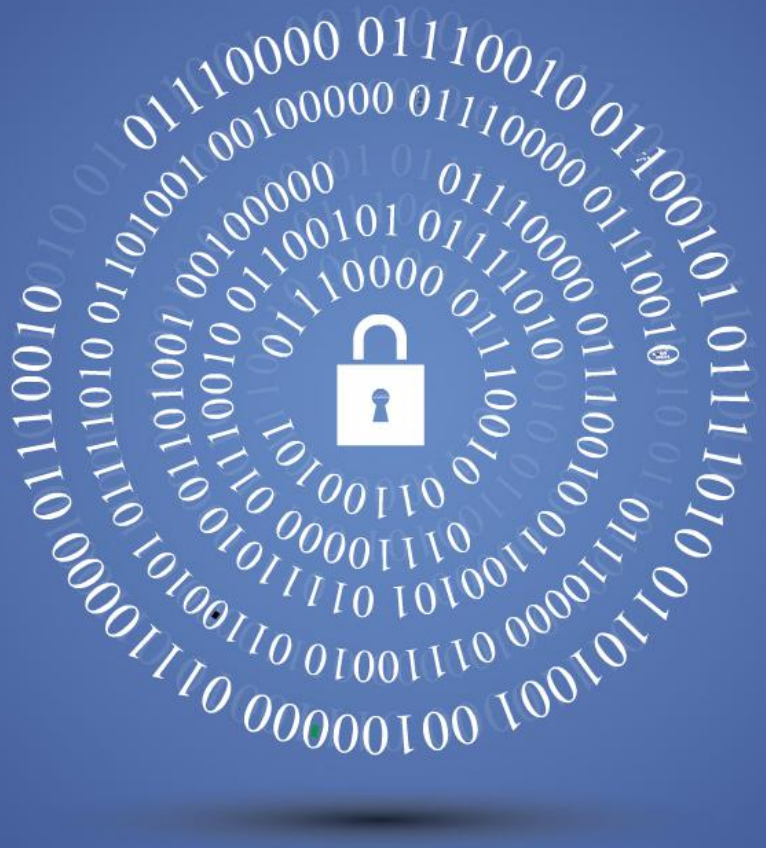
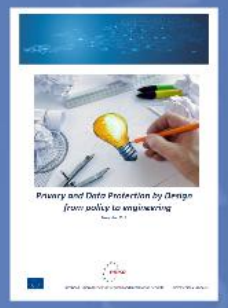



Privacy by Design & Default
Data Protection Impact Assessment

Design & Default



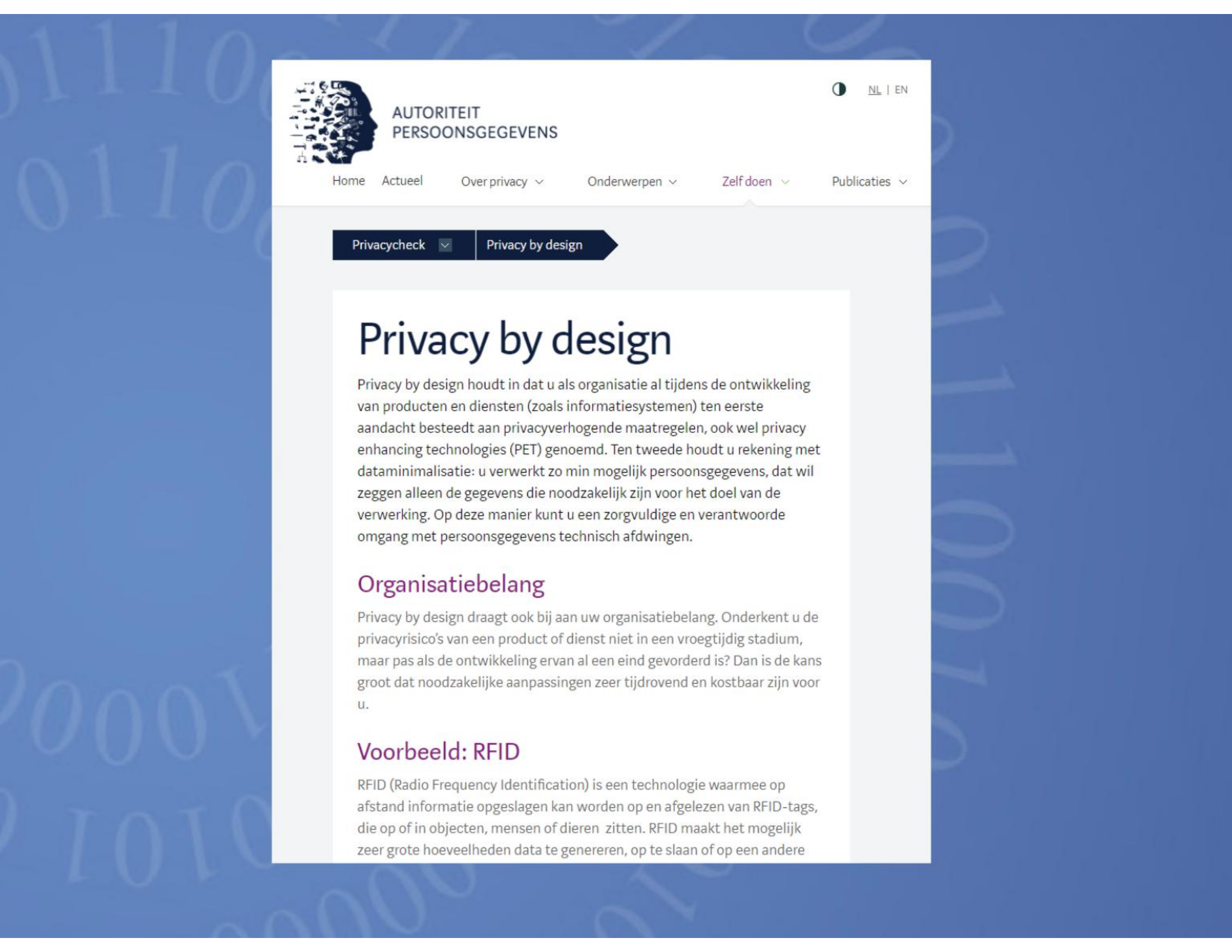
Artikel 25

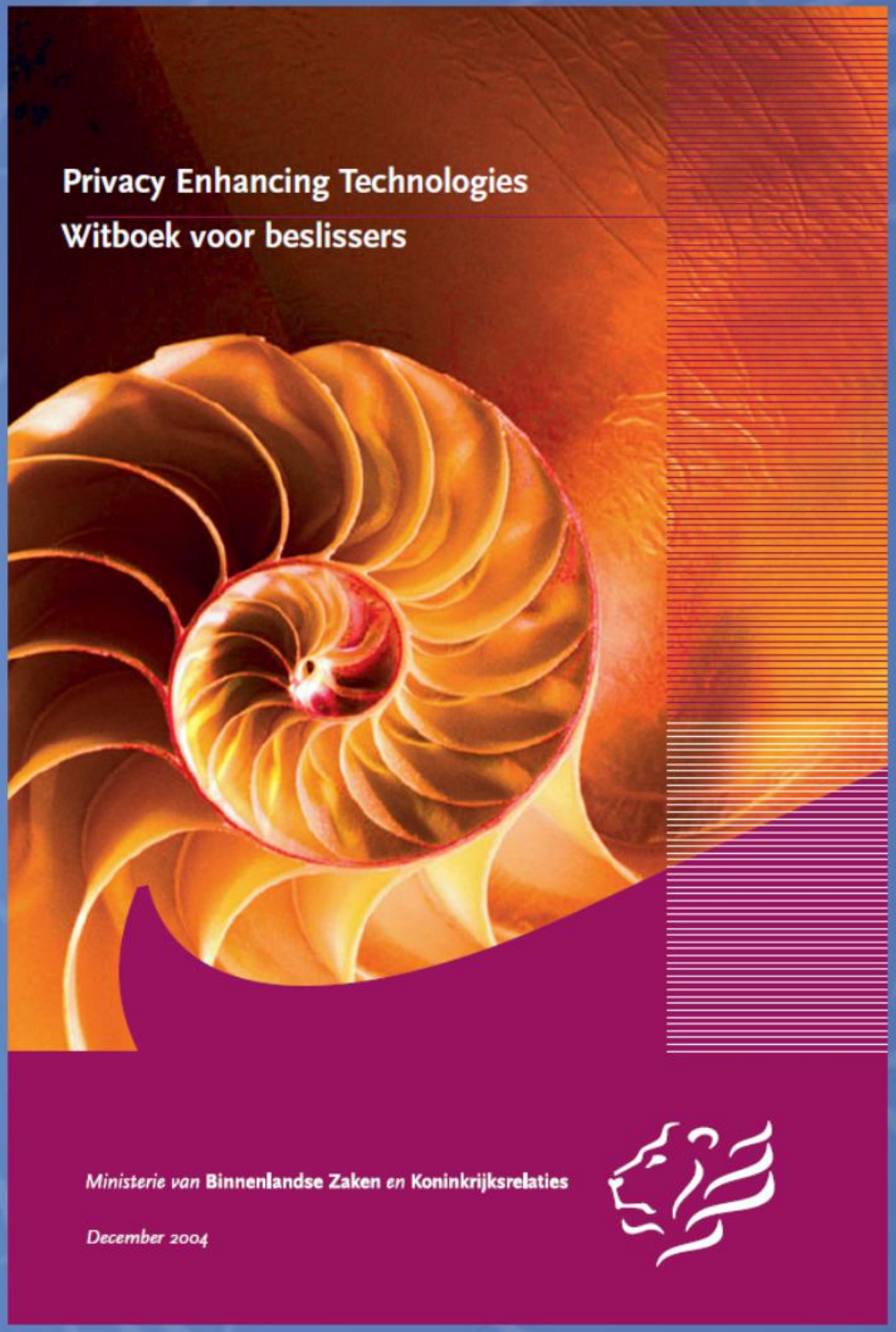
Gegevensbescherming door ontwerp en door standaardinstellingen

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

3. Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.


AUTORITEIT
PERSOONSGEGEVENS
NL | EN
Home
Actueel
Over privacy
Onderwerpen
Zelf doen
Publicaties
Privacycheck
Privacy by design
Privacy by design
Privacy by design houdt in dat u als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op deze manier kunt u een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen.
Organisatiebelang
Privacy by design draagt ook bij aan uw organisatiebelang. Onderkent u de privacyrisico's van een product of dienst niet in een vroegtijdig stadium, maar pas als de ontwikkeling ervan al een eind gevorderd is? Dan is de kans groot dat noodzakelijke aanpassingen zeer tijdrovend en kostbaar zijn voor u.
Voorbeeld: RFID
RFID (Radio Frequency Identification) is een technologie waarmee op afstand informatie opgeslagen kan worden op en afgelezen van RFID-tags, die op of in objecten, mensen of dieren zitten. RFID maakt het mogelijk zeer grote hoeveelheden data te genereren, op te slaan of op een andere


Privacy Enhancing Technologies
Witboek voor beslissers
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
December 2004

Voor een grondige totaalbenadering, met uitgangspunten die doorgaans uit andere richtsnoeren en wettelijke en reglementaire voorschriften komen (bijv. IDW PS 330, BOBIT, ISO 27001), volgt PbD in de vorm van een geclassificeerd model:

- bedrijfsprocessen
- ondersteunende IT-systemen en toepassingen, en
- fysieke en technische ontwerpen en online infrastructuren.

De principes van Privacy by Design zijn daarbij toepasbaar op alle soorten persoonlijke informatie. De kwaliteit en de diepgang van de omzetting en de effectiviteit van de noodzakelijke privacymaatregelen moeten daarbij aansluiten op de risicogevoeligheid en de behoefte aan beveiliging.

Doelen en de zeven principes van PbD

De doelen van PbD - volgens Cavoukian de waarborg van privacybescherming - zijn 'persoonlijke controle over de eigen gegevens' en 'het gewin van een duurzaam concurrentievoordeel voor organisaties'. Deze zijn haalbaar door 7 basisprincipes te volgen:

- Voorkomen is beter dan genezen
- Dataprotectie is standaard
- Integreren van gegevensbescherming en beveiliging in het design
- Volledige functionaliteit - een positieve balans
- Bescherming gedurende de hele levenscyclus
- Zichtbaarheid en transparantie
- Respect voor de privacy van de gebruiker

In 2007 pakte het Europees Parlement het concept van PbD voor het eerst op, met als gevolg dat de EU-Commissie het in 2012 verwerkte in het ontwerp van het dataprotectieverdrag.

PROFIELEN

BIT, ISO

en de

lgen:

gevolg
g.

Privacy and Data Protection by Design – from policy to engineering

December 2014

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu

Privacy by Design
The 7 Foundational Principles
Implementation and Mapping of Fair Information Practices

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner, Ontario, Canada

Purpose:

This document provides readers with additional information, clarification and guidance on applying the 7 Foundational Principles of *Privacy by Design (PbD)*.

This guidance is intended to serve as a reference framework and may be used for developing more detailed criteria for application and audit/verification purposes.

Scope:

These information management principles − and the philosophy and methodology they express − can apply to specific technologies, business operations, physical architectures and networked infrastructure, and even to entire information ecosystems and governance models.

The universal principles of the Fair Information Practices (FIPs) are affirmed by those of *Privacy by Design*, but go beyond them to seek the highest global standard possible. Extending beyond FIPs, *PbD* represents a significant "raising" of the bar in the area of privacy protection.

Context:

With the shift from industrial manufacturing to knowledge creation and service delivery, the value of information and the need to manage it responsibly have grown dramatically. At the same time, rapid innovation, global competition and increasing system complexity present profound challenges for informational privacy.

While we would like to enjoy the benefits of innovation − new conveniences and efficiencies − we must also preserve our freedom of choice and personal control over our data flows. Always a social norm, privacy has nonetheless evolved over the years, beyond being viewed solely as a legal compliance requirement, to also being recognized as a market imperative and critical enabler of trust and freedoms in our present-day information society.

There is a growing understanding that innovation, creativity and competitiveness must be approached from a "design-thinking" perspective − namely, a way of viewing the world and overcoming constraints that is at once holistic, interdisciplinary, integrative, innovative, and inspiring.

Privacy, too, must be approached from the same design-thinking perspective. Privacy must be incorporated into networked data systems and technologies, **by default**. Privacy must become integral to organizational priorities, project objectives, design processes, and planning operations. Privacy must be

embedded into every standard, protocol and process that touches our lives. This document seeks to make this possible by striving to establish a universal framework for the strongest protection of privacy available in the modern era.

The 7 Foundational Principles of Privacy by Design are presented below ***in Bold,*** followed by the FIPs principles that map onto each one.

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred − it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

Whether applied to information technologies, organizational practices, physical design, or networked information ecosystems, *PbD* begins with an explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently (for example, preventing (internal) data breaches from happening in the first place). This implies:

- A clear commitment, at the highest levels, to set and enforce high standards of privacy − generally higher than the standards set out by global laws and regulation.
- A privacy commitment that is demonstrably shared throughout by user communities and stakeholders, in a culture of continuous improvement.
- Established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways.

2. Privacy as the ***Default***

We can all be certain of one thing − the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy − it is built into the system, by default.

This *PbD* principle, which could be viewed as **Privacy by Default,** is particularly informed by the following FIPs:

- **Purpose Specification** – the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.
- **Collection Limitation** – the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.
- **Data Minimization** − the collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

- **Use, Retention, and Disclosure Limitation** – the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

Where the need or use of personal information is not clear, there shall be a presumption of privacy and the precautionary principle shall apply: the default settings shall be the most privacy protective.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrative and creative way. Holistic, because additional, broader contexts must always be considered. Integrative, because all stakeholders and interests should be consulted. Creative, because embedding privacy sometimes means re-inventing existing choices because the alternatives are unacceptable.

- A systemic, principled approach to embedding privacy should be adopted − one that relies upon accepted standards and frameworks, which are amenable to external reviews and audits. All fair information practices should be applied with equal rigour, at every step in the design and operation.

- Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks and all measures taken to mitigate those risks, including consideration of alternatives and the selection of metrics.

- The privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration or error.

4. **Full** Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

Privacy by Design does not simply involve the making of declarations and commitments − it relates to satisfying all legitimate objectives − not only the privacy goals. *Privacy by Design* is doubly-enabling in nature, permitting full functionality − real, practical results and beneficial outcomes to be achieved for multiple parties.

- When embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired, and to the greatest extent possible, that all requirements are optimized.

- Privacy is often positioned in a zero-sum manner as having to compete with other legitimate interests, design objectives, and technical capabilities, in a given domain. *Privacy by Design* rejects taking such

an approach – it embraces legitimate non-privacy objectives and accommodates them, in an innovative positive-sum manner.

- All interests and objectives must be clearly documented, desired functions articulated, metrics agreed upon and applied, and trade-offs rejected as often being unnecessary, in favour of finding a solution that enables multi-functionality.

Additional recognition is garnered for creativity and innovation in achieving all objectives and functionalities in an integrative, positive-sum manner. Entities that succeed in overcoming outmoded zero-sum choices are demonstrating first-class global privacy leadership, having achieved the Gold Standard.

5. End-to-End Security – Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

Privacy must be continuously protected across the entire domain and throughout the life-cycle of the data in question. There should be no gaps in either protection or accountability. The "Security" principle has special relevance here because, at its essence, without strong security, there can be no privacy.

- **Security** − Entities must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire lifecycle, consistent with standards that have been developed by recognized standards development bodies.

- **Applied security** standards must assure the confidentiality, integrity and availability of personal data throughout its lifecycle including, *inter alia*, methods of secure destruction, appropriate encryption, and strong access control and logging methods.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!

Visibility and transparency are essential to establishing accountability and trust. This PbD principle tracks well to Fair Information Practices in their entirety, but for auditing purposes, special emphasis may be placed upon the following FIPs:

- **Accountabilty** – The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured.

- **Openness** – Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

- **Compliance** – Complaint and redress mechanisms should be established, and information communicated about them to individuals, including how to access the next level of appeal. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should be taken.

7. Respect for User Privacy

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!

The best *Privacy by Design* results are usually those that are consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data.

Empowering data subjects to play an active role in the management of their own data may be the single most effective check against abuses and misuses of privacy and personal data. Respect for User Privacy is supported by the following FIPs:

- **Consent** – The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

- **Accuracy** – personal information shall be as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

- **Access** – Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

- **Compliance** – Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal.

Respect for User Privacy goes beyond these FIPs, and extends to the need for human-machine interfaces to be human-centered, user-centric and user-friendly so that informed privacy decisions may be reliably exercised. Similarly, business operations and physical architectures should also demonstrate the same degree of consideration for the individual, who should feature prominently at the centre of operations involving collections of personal data.

+++

Further information and all references at: www.privacybydesign.ca

Data Protection Impact Assessment

Afdeling 3

Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging

Artikel 35

Gegevensbeschermingseffectbeoordeling

1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

2. Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.

3. Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:

a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;

b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of

c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

4. De toezichthoudende autoriteit stelt een lijst op van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling overeenkomstig lid 1 verplicht is, en maakt deze openbaar. De toezichthoudende autoriteit deelt die lijsten mee aan het in artikel 68 bedoelde Comité.

5. De toezichthoudende autoriteit kan ook een lijst opstellen en openbaar maken van het soort verwerking waarvoor geen gegevensbeschermingseffectbeoordeling is vereist. De toezichthoudende autoriteit deelt deze lijst mee aan het Comité.

6. Wanneer de in de leden 4 en 5 bedoelde lijsten betrekking hebben op verwerkingen met betrekking tot het aanbieden van goederen of diensten aan betrokkenen of op het observeren van hun gedrag in verschillende lidstaten, of op verwerkingen die het vrije verkeer van persoonsgegevens in de Unie wezenlijk kunnen beïnvloeden, past de bevoegde toezichthoudende autoriteit voorafgaand aan de vaststelling van die lijsten het in artikel 63 bedoelde coherentiemechanisme toe.

7. De beoordeling bevat ten minste:

a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;

b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;

c) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en

d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

8. Bij het beoordelen van het effect van de door een verwerkingsverantwoordelijke of verwerker verrichte verwerkingen, en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van de in artikel 40 bedoelde goedgekeurde gedragscodes naar behoren in aanmerking genomen.

9. De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.

10. Wanneer verwerking uit hoofde van artikel 6, lid 1, onder c) of e), haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is, de specifieke verwerking of geheel van verwerkingen in kwestie daarbij wordt geregeld, en er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een gegevensbeschermingseffectbeoordeling is uitgevoerd, zijn de leden 1 tot en met 7 niet van toepassing, tenzij de lidstaten het noodzakelijk achten om voorafgaand aan de verwerkingen een dergelijke beoordeling uit te voeren.

11. Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

AUTORITEIT PERSOONSGEGEVENS

NL | EN

Doorzoek de gehele site

TIP ONS

Home Actueel Over privacy Onderwerpen Zelf doen Publicaties Melden

Privacycheck | Privacy impact assessment (PIA)

Privacy impact assessment (PIA)

Wilt u als organisatie privacyrisico's van een project in een vroeg stadium op een gestructureerde en heldere manier in beeld brengen? Dan kunt u een privacy impact assessment (PIA) (laten) uitvoeren.

Een PIA stimuleert u om op tijd na te denken over vragen als:

- wat de impact is van het beoogde project op de privacy van de betrokkenen (de mensen van wie u persoonsgegevens verwerkt);
- wat de risico's zijn voor de betrokkenen en voor de organisatie;
- of er, gegeven de doelstellingen van het project, ook een aanpak mogelijk is die minder gevolgen heeft voor de privacy.

Doelen PIA

Met een PIA kunt u het volgende bereiken:

- minder gevolgen van toezicht en handhaving;
- betere kwaliteit gegevens;
- betere dienstverlening;
- betere besluitvorming;

Publicaties

Wetgevingsadvies / 5 maart 2013

PDF

Advies - concept toetsmodel Privacy Impact Assessment

DOWNLOADEN

	Vragen	Antwoord (ja/nee)	Indien van toepassing: Aanvullende toelichting op het antwoord	Resulteert het antwoord in een mogelijk risico? (ja/nee)	Omschrijving van het risico (zowel wanneer het antwoord ja of nee is)
	PB-Light		PB-Light		PB-Light
	Algemene informatie over de verwerking van persoonsgegevens				
I	Welke persoon / rol is verantwoordelijk voor het proces, systeem, applicatie, database of project?		*Noteer hier de namen.*		N.V.T.
II	Wie vult deze PB in?		*Noteer hier de namen.*		N.V.T.
III	Op welke datum is deze PB uitgevoerd en op welke datum dient de PB te worden geactualiseerd?		*1. Noteer hier de datum.* *2. Noteer hier de uiterste actualisatiedatum:*		N.V.T.
IV	Geef een korte omschrijving van het proces, systeem, applicatie, database of project.		*1. Noteer hier een algemene beschrijving van het proces, systeem, applicatie, database of project.* *2. Voeg daarnaast achtergrondinformatie toe door middel van het toevoegen van bestanden aan deze PB.* *3. Voeg een visueel stroomschema toe aan deze PB.*		N.V.T.
	1. Vaststellen verantwoordelijke.				
1.1	Is het duidelijk wie de verantwoordelijke is voor de verwerking van de persoonsgegevens?		*Indien PostNL als verantwoordelijke kan worden aangemerkt, ga door naar vraag 2.1.*	Ja	Risico (Indien het antwoord nee is): Doordat niet bekend is wie de verantwoordelijke is voor de verwerking van persoonsgegevens, bestaat het risico dat niemand zich gehouden voelt om de privacyregels toe te passen, waardoor de bescherming van de persoonsgegevens mogelijk niet (voldoende)
	2. Categorieën persoonsgegevens.				
	NAW-gegevens	0			
	Telefoonnummer	0			
	E-mailadres	0			
	Geboortedatum	0			
	Personeelsnummer (Een code of nummer dat te herleiden is naar de medewerker.)	0			
	Financiële persoonsgegevens (Bijvoorbeeld bankrekeningnummers.)	0			
	Overige persoonsgegevens (Dit betreft alle gegevens die niet vallen onder de hier genoemde categorieën, maar alleen of in combinatie wel te herleiden zijn naar een persoon. Voorbeelden zijn social media-pagina's of een IP-adres.)	0			
2.2	Van welke categorie betrokkenen worden persoonsgegevens verwerkt?		*Consumenten* *Zakelijke klanten (B2B)* *Werknemer (of informatie gerelateerd aan)* *Sollicitanten* *Leveranciers* *Overig*		Risico (Indien het antwoord overig is): Door geen zicht te hebben op de categorieën betrokkenen van wie persoonsgegevens worden verwerkt, kunnen niet de juiste risico's worden ingeschat en daarmee niet passende privacy verhogende maatregelen worden genomen.
	3. Grondslag				
3.1	Vanuit welke grondslagen (wettelijke toegestane reden) gaat of vindt de verwerking van persoonsgegevens plaats? (Geef aan met Ja/Nee)		A. De betrokkene heeft toestemming gegeven voor de verwerking van zijn of haar persoonsgegevens voor een of meer specifieke doeleinden.	0	


Wet bescherming persoonsgegevens
Samenwerkingsverband Audit Aanpak / Werkgroep Zelfevaluatie
WBP Zelfevaluatie

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 248

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Adopted on 4 April 2017

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

Informatiebeveiliging en meldplicht datalekken

Persoonsgegevensbeveiliging

Artikel 32

Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

4. De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.

COLLEGE BESCHERMING PERSOONSGEGEVENS

CBP Richtsnoeren

BEVEILIGING VAN PERSOONSGEGEVENS

FEBRUARI 2013

POSTADRES Postbus 93374, 2509 AJ Den Haag
TEL 070 - 88 88 500 **FAX** 070 - 88 88 501

De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)

Beleidsregels voor toepassing van artikel 34a van de Wbp

DATUM 8 december 2015

Sterke relatie met 'business continuity plans' (IT aanvallen en datalekken)

zodat de kans hierop vermindert:

Investeer pro actief in 'data ethics'

It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.

Warren Buffett