Hekkelman advocaten | notarissen

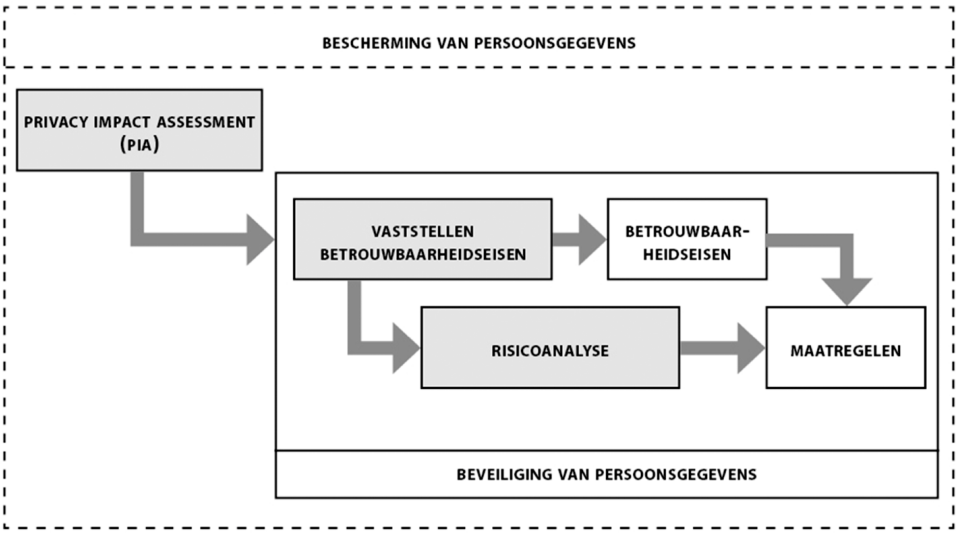
Checklist Beveiliging Persoonsgegevens

Beveiliging is een één van de belangrijkste vereisten binnen het privacyrecht. Iedere organisatie zal passende technische en organisatorische maatregelen moeten treffen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Daarvoor zal een beveiligingsbeleid inclusief betrouwbaarheidseisen (BIV: beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens) moeten zijn vastgesteld dat betrekking heeft op alle verwerkingen van persoonsgegevens binnen de organisatie. Ook zal bij gebruik van een nieuwe technologie, een aanpassing in de bestaande systemen of indien de verwerking wordt uitbesteed, een afzonderlijke Plan-Do-Check-Act cyclus (PDCA) doorlopen moeten worden. Hieronder eerst de stappen voor een ondernemingsbreed beveiligingsbeleid en vervolgens voor een specifieke PDCA.

Fase 1: Opstellen ondernemingsbreed beveiligingsbeleid

Ook het ondernemingsbreed beveiligingsbeleid zal moeten worden opgesteld in de vorm van een PDCA.

STAP 1: "PLAN"[1]



Inventarisatie

In kaart brengen van alle gegevensstromen (personeel, klanten, prospects)

Wie zijn de schakels in de keten (verstrekkers, ontvangers, gebruikers, interne bewerkers, bewerkers en subbewerkers)

Uitvoeren van een formele risicoanalyse

[1] Bron: CBP Richtsnoeren Beveiliging Persoonsgegevens, p.17

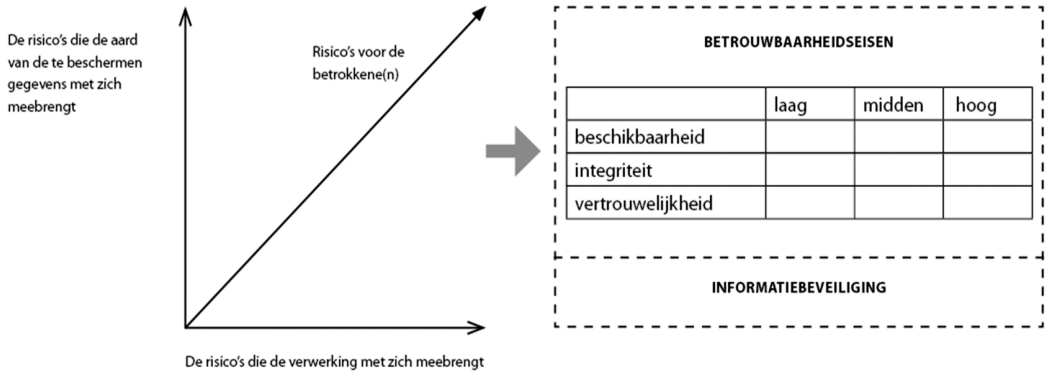
Hekkelman advocaten | notarissen

Al dan niet gebruik van een Privacy Impact Assesment (PIA) voorschrijven om de risico's te beoordelen

Nagaan of het beveiligingsbeleid erop is gericht om alle verwerkingen af te dekken

Vaststellen betrouwbaarheidseisen (BIV-waarden[2])

Zijn de ondernemingsbrede betrouwbaarheidseisen voor alle verwerkingen vastgesteld (eisen aan het niveau van beschikbaarheid, integriteit en vertrouwelijkheid "BIV-waarden")



De betrouwbaarheidseisen worden vastgesteld door de gevolgen voor de betrokkenen te bepalen bij verlies, corruptie of onrechtmatige verwerking van hun persoonsgegevens.
Voorbeeld: bij een ziekenhuis informatie systeem is essentieel dat patiëntgegevens onmiddellijk beschikbaar zijn, dat deze volledig en juist zijn en dat de vertrouwelijkheid goed geborgd is. De BIV-waarden worden dan 3.3.3. (= hoog-hoog-hoog).

Onderscheid maken naar de aard van persoonsgegevens:

"Bijzondere persoonsgegevens": godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakbond en strafrechtelijke gegevens

Persoonsgegevens van vertrouwelijke aard: financieel of economisch (schulden), stigmatiserend (verslaving, naaktfoto's, specifieke problemen), inloggegevens, gegevens die bruikbaar zijn voor identiteitsfraude (kopie ID, BSN, handtekening, biometrische gegevens), gegevens die vallen onder beroepsgeheim, koersgevoelige informatie of bedrijfsgeheimen

Rekening houden met de kwetsbaarheid van bepaalde groepen (zieken, kinderen)

[2] Bron: CBP Richtsnoeren Beveiliging Persoonsgegevens, p.18

Hekkelman advocaten | notarissen

Risicoanalyse

Verricht een risicoanalyse rekening houdend met de vastgestelde betrouwbaarheidseisen en de aard van de persoonsgegevens.

In het ondernemingsbreed beveiligingsbeleid onder meer aandacht besteden aan:

- De verdeling van verantwoordelijkheden voor informatiebeveiliging
- Beveiligingsbewustzijn (werkinstructies en trainingen)
- Continuïteitseisen (back up en restore policy)
- Beveiligingsstandaarden en richtlijnen van het Nationaal Cyber Security Center
- Selectiecriteria voor leveranciers
- Softwareontwikkeling en/of ontwikkeling van apps
- Gegevens in e-mailsystemen (opslag/transport)
- Controle op en screening van medewerkers
- Bepalingen in arbeidsovereenkomsten (geheimhoudingsbepalingen)
- Specifiek karakter cloud-toepassingen
- Procedures handhaving bewaartermijnen
- Aanwezigheid controlemechanismen

STAP 2: "DO"

Schrijf beveiligingsmaatregelen voor per categorie van verwerking

Mogelijke beveiligingsmaatregelen die kunnen worden voorgeschreven:

- Toepassen privacy by design en privacy by default
- Opstellen bewustwordingsprogramma voor personeel en ingeschakelde derden
- Fysieke beveiliging persoonsgegevens en gegevensdragers
- Toegangsbeveiliging, beveiliging verbindingen en beveiliging gegevens (autorisaties, versleuteling, hashing, privacy by default)
- Logging van toegang tot vertrouwelijke gegevens (wie heeft toegang gehad tot gegevens)
- Volg actuele beveiligingsstandaarden die betrekking hebben op de verwerkte persoonsgegevens (bijvoorbeeld vigerende Code voor informatiebeveiliging NEN-ISO 27002 en voor de zorgsector NEN 7510) en de NCSC richtlijnen
- Maatregelen om vooraf de gevolgen van een eventueel beveiligingsincident te beperken (pseudonimiseren, versleutelen, remote wissen)
- Maatregelen om beveiligingsincidenten te detecteren (logging, geautomatiseerde controle op hacks, malware e.d.)
- Opzetten procedure en aanwijzen verantwoordelijke voor incidentenbeheer en de opvolging van beveiligingsincidenten (waaronder meldplicht datalekken)

Hekkelman advocaten | notarissen

- Inrichten continuïteitsbeheer[3] bij calamiteiten (brand datacenter, faillissement bewerker, uitval apparatuur)
- Geheimhoudingsafspraken intern en extern
- Beveiligingsafspraken in bewerkerscontracten (beveiligingseisen, geheimhouding, incidentenbeheer, controle)
- Opzetten controlesysteem naleving beveiligingsbeleid

STAP 3: "CHECK"

Controle op organisatorische maatregelen

- Controle omgang met persoonsgegevens via werkplekcontroles
- Controle naleving werkinstructies bijvoorbeeld door "social engineering tests"
- Content filtering telefoon/e-mail/internet

Controle op technische maatregelen

- Controle up to date zijn gebruikte programmacodes (stand van de techniek)
- Testen van de gebruikte informatiesystemen (penetratietest)
- Uitvoeren van beveiligingsassessments (al dan niet door een onafhankelijke expert of RE auditor)

Controle bij uitbesteding

- Recht om zelf te (laten) controleren bij derde
- Periodieke rapportages van onafhankelijke derden over continuïteit van de verwerking en de kwaliteit van de beveiliging

Periodieke evaluatie effectiviteit van het ondernemingsbreed beveiligingsbeleid

- Nagaan of de bestaande maatregelen in geval van veranderingen in de organisatie nog voldoen
- Nagaan of bij wijziging van gebruikte systemen of bij aanschaf van nieuwe systemen de vastgestelde betrouwbaarheidseisen in het beveiligingsbeleid toereikend zijn
- Periodiek nagaan of de betrouwbaarheidseisen nog aansluiten bij de risico's die alle verwerkingen en de aard van de persoonsgegevens meebrengen

STAP 4: "ACT"

Maatregelen nemen naar aanleiding van tekortkomingen uit stap 3

Aanpassing beveiligingsbeleid aan de hand van de uitkomsten van de controles

[3] ook het verloren gaan van persoonsgegevens valt onder het begrip "inbreuk op de beveiliging" en de meldplicht datalekken

Hekkelman advocaten | notarissen

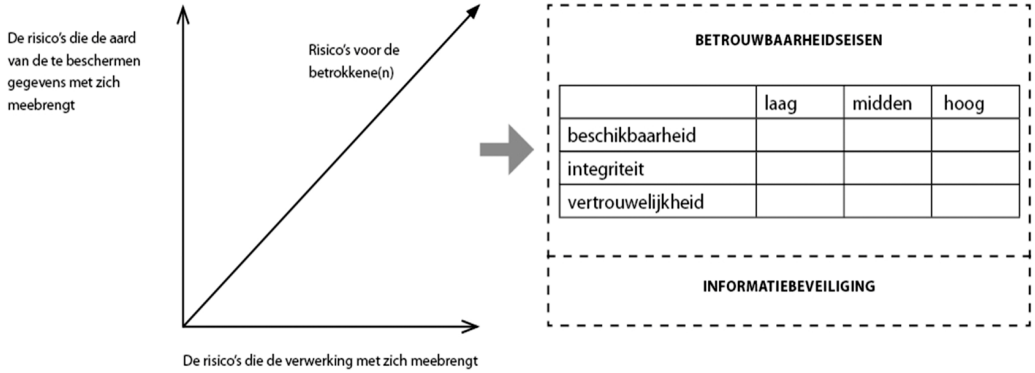
Fase 2: Projectniveau

Ook bij een aanpassing van een bestaande verwerking, zoals gebruiken van een nieuw systeem, of verwerking in de cloud, dan wel de introductie van een nieuwe verwerking, zal een PDCA aanpak moeten worden gevolgd.

STAP 1: "PLAN"

Uitvoeren van een risicoanalyse, rekening houdend met de specifieke kenmerken van de verwerking en gebruikte technologie

Stel de specifieke betrouwbaarheidseisen vast voor de verwerking of het informatiesysteem (BIV-waarden)[4]



Inventariseer de bedreigingen die kunnen leiden tot een beveiligingsincident

Stap 2: "DO"

Tref passende beveiligingsmaatregelen die waarborgen dat aan de vastgestelde betrouwbaarheidseisen uit het ondernemingsbreed beveiligingsbeleid en eventuele specifieke aanvullende eisen wordt voldaan
Documenteer de getroffen maatregelen

Stap 3: "CHECK"

Controleer of de maatregelen daadwerkelijk getroffen zijn, worden nageleefd en toereikend zijn om aan de vastgestelde betrouwbaarheidseisen te voldoen

[4] Bron: CBP Richtsnoeren Beveiliging Persoonsgegevens, p.18

Hekkelman advocaten | notarissen

Stap 4: “ACT”

Ga na of de bestaande maatregelen nog voldoen en de betrouwbaarheidseisen nog toereikend zijn en tref maatregelen aan de hand van de uitkomsten van de controle

Monique Hennekens

Hekkelman Advocaten N.V.
T 024 - 382 83 29
M 06 - 281 393 87
m.hennekens@hekkelman.nl