NVIA

Data | Modellen | Privacy

PIM POPPE

September 2017

PROBABILITY
& PARTNERS

Wat aan de orde komt

1. Introductie
2. Algemene verordening gegevensbescherming (AVG)
3. Belangrijkste Implicaties
4. Lessen van andere veranderingen in regelgeving
5. Conclusies

Pim Poppe

Even voorstellen:

- Macro economie, UvA
- Directeur Group Risk Management, Robeco, 1996 – 2004
- Directeur Group Risk Management, SNS REAAL, 2004 – 2013
- Probability & Partners, vanaf oktober 2014

Doel van vandaag:

- Dialoog. Nog geen antwoorden

Wat is Probability & Partners?

- Risk Management-adviesbureau gestart in 2014

Wat onderscheidt ons:

✓ Integrale benadering en verbinding tussen risico-domeinen

✓ Verbinding tussen consultancy en implementatie

Expertise domeinen:

- Financieel Risico management, Operational Risk, Compliance, Security (Gouda)
- Modelbouw, Modelvalidatie (Amsterdam)

Diensten en doelmarkten

PROBABILITY & PARTNERS

Doelmarkten	Klanten	Thema`s	Regulatory Change	Diensten
Pensioenen		A. Integraal Risico Management B. Uitbesteding C. Flexibiliteit / Ontbundeling D. Governance E. Risk Reporting F. Cyber Crime G. Model Risk	1. nFTK / IORP II 2. GDPR / AVG 3. Solvency II 4. MIFID II 5. PERDARR 6. FRTB 7. CRD 8. CRR 9. BASEL II	Risk Consultancy
Verzekeren				Managed Service Risk
Banken				Interim
Overig				Change / Projecten

Algemene verordening gegevensbescherming

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?

- De AVG zorgt onder meer voor:
- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor organisaties;
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

Voorbereiding op AVG volgens AP

1. Bewustwording
2. Rechten van betrokkenen
3. Overzicht verwerkingen
4. Data protection impact assessment (DPIA)
5. Privacy by design & privacy by default
6. Functionaris voor de gegevensbescherming
7. Meldplicht datalekken
8. Bewerkersovereenkomsten
9. Leidende toezichthouder
10. Toestemming

Wat kan verwerken zijn?

- verzamelen
- vastleggen
- ordenen
- bewaren
- bijwerken
- wijzigen
- opvragen
- raadplegen
- gebruiken
- doorzenden
- verspreiden
- beschikbaar stellen
- samenbrengen
- met elkaar in verband brengen
- uitwissen
- vernietigen

Rechten Betrokkene

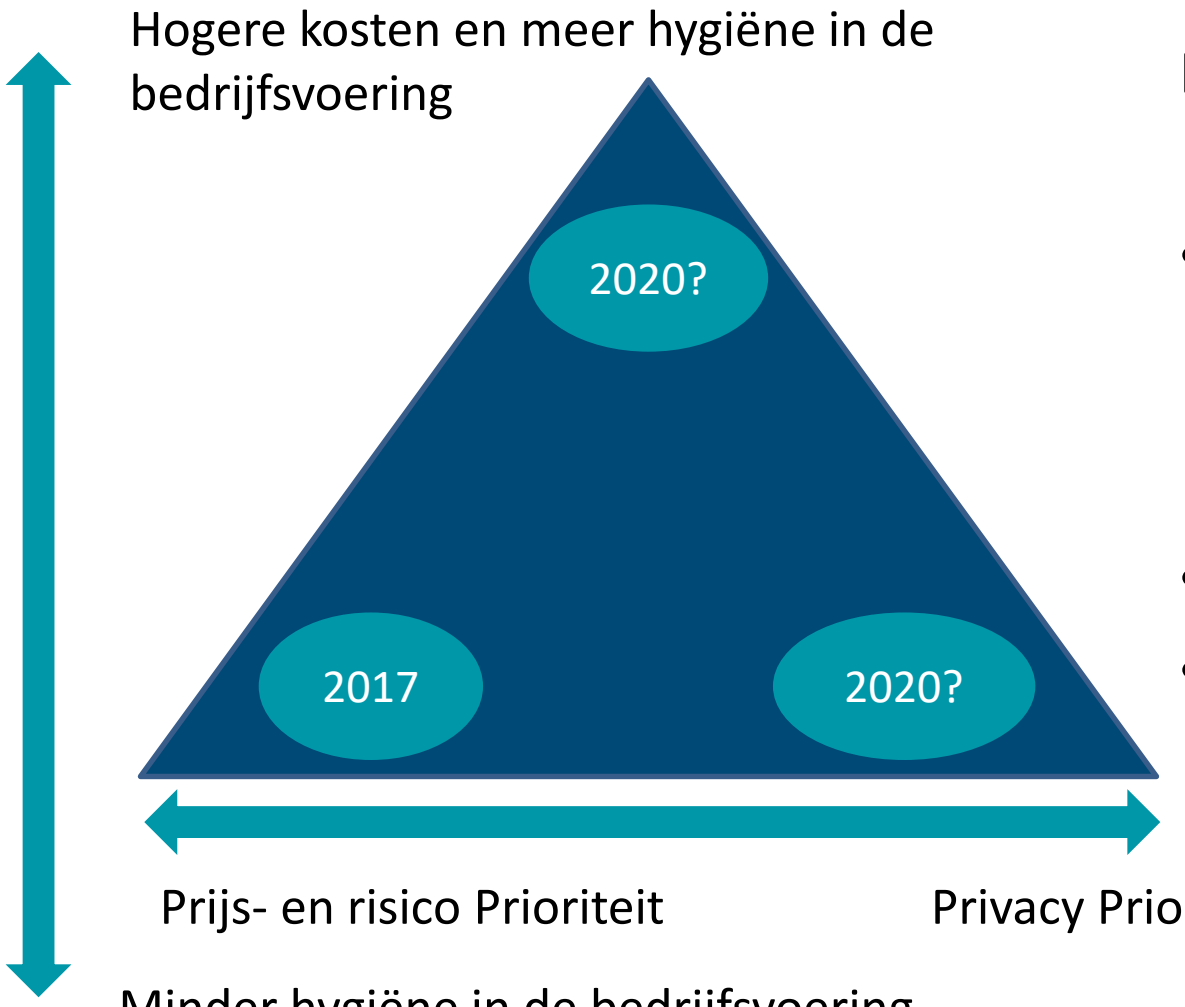
Werknemer is ‘betrokkene’ in AVG-begrippenkader

Deze heeft meer rechten:

- Toestemming
- Recht op persoonsgegevens verwijderen
- Recht op inzage
- Recht op portabiliteit
- Recht op bezwaar
- Recht op vergetelheid

De organisaties moeten zich voorbereiden om deze rechten op een goede manier te faciliteren. Beleid maken, Procedure en Processen aanpassen, IT op orde brengen.

Balanceer-oefening



Er is een uitruil tussen:

- Het niet goed in kunnen schatten van Risico's en prijzen (arme data en modellen)
- Het niet voldoen aan AVG
- Kosten implementatie

Paralellen met andere trajecten

Nieuwe regelgeving met invloed op data en modellen =

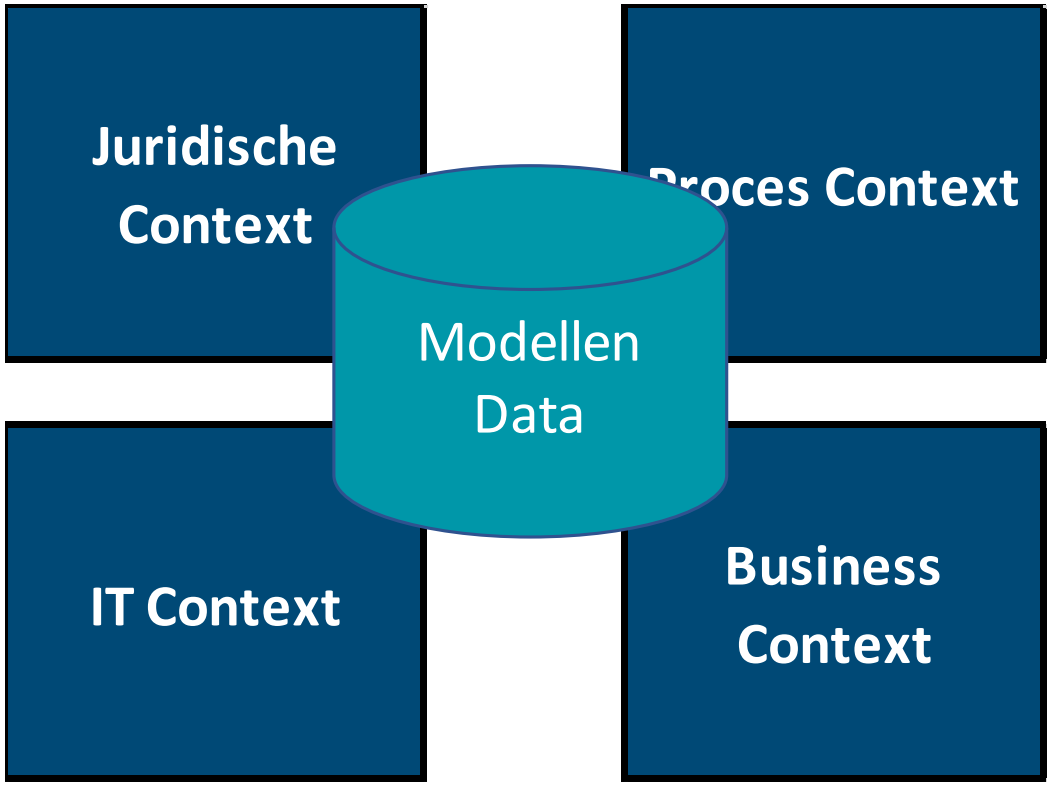
Implementatiekosten + nieuwe prikkels + business impact

- <u>Voorbeelden</u>
- Basel II
- IFRS9
- Solvency II
- Basel III
- GIPS AIMR

<u>Lessen</u>

- In het begin verschillende opvattingen over de juiste implementatie
- Te snel implementeren heeft kosten en te langzaam ook
- Onbedoelde bij-effecten
- Het duurt ongeveer vijf jaar voordat de implementatie is afgerond

Contexten



- Er zijn verschillende contexten waarbinnen je naar de AVG kan kijken.
- Gebruik iedere context (bril) op een gepaste wijze.

Juridische Context: Wbp

- **Belangrijkste bepalingen Wbp**
- De belangrijkste bepalingen uit de Wbp over het rechtmatig omgaan met persoonsgegevens zijn als volgt samen te vatten:
- Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt.
- Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.
- Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking.
- De gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

Bron AP

Juridische context: Wpb naar AVG

Veranderingen per 25 mei 2018

Per 25 mei 2018, als de AVG van toepassing is, verandert er onder meer het volgende voor organisaties:

- zij hoeven verwerkingen van persoonsgegevens niet meer te melden bij de Autoriteit Persoonsgegevens;
- zij kunnen verplicht zijn een data protection impact assessment (DPIA) uit te voeren;
- zij kunnen verplicht zijn een functionaris voor de gegevensbescherming aan te stellen.

Bron AP

Implicatie……

Juridische Context: Verantwoording

Verantwoordingsplicht

Organisaties hebben daarom een verantwoordingsplicht. Dit houdt in dat zij met documenten moeten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG te voldoen.

Bron AP

Implicatie……

Juridische Context GPDR en AP

Jurisprudentie

Een wet kan nooit alles regelen. Er zijn altijd uitzonderingen en twijfelgevallen. In praktijk zal moeten blijken hoe rechters in de EU oordelen over individuele privacy kwesties.

Bron AP

Implicatie……

Proces Context

- De life cycle van persoonsgegevens moet worden uitgeschreven.
- We vraagt wat wanneer uit?
- Op welk moment worden gegevens geanonimiseerd?
- Wanneer verwijderden onder wiens verantwoordelijkheid?
- Hoe leggen we de doelen vast waarom de data wordt vastgelegd?
- Hoe zorgen we dat de data niet voor andere doelen worden gebruikt?
- etc

Proces context - Wat kan verwerken zijn?

- verzamelen
- vastleggen
- ordenen
- bewaren
- bijwerken
- wijzigen
- opvragen
- raadplegen
- gebruiken
- doorzenden
- verspreiden
- Beschikbaar stellen
- samenbrengen
- met elkaar in verband brengen
- uitwissen
- vernietigen

IT Context

- De nieuwe processen, data beveiligingsclassificatie, bescherming van data zullen tot extra inspanningen leiden.

- Aantoonbaarheid van security en compliance met de privacy regels vragen om zwaardere IT-implementatie.

- Complicerende factor daarbij is dat er meerdere ‘hand-overs’ zijn van de data tussen verschillende partijen.

- Bij alle nieuwe initiatieven moet beoordeeld worden wat de consequenties zijn voor de nieuwe rechten een vrijheden van individuen. Dit moet in processen en systemen bij het ontwerp reeds worden verankerd (privacy by design).

Business Context

- Bewustwording vraagt expliciete aandacht, opleiding, training. Kost business uren
- De belemmeringen om data vast te leggen en te bewerken zal de mogelijkheden beïnvloeden risico's te kwantificeren om goed prijzen
- Mogelijk worden premies minder risico gerelateerd
- Mogelijk gaan de opslagen voor onzekerheid in de premies omhoog
- De hygiëne gaat zeker geld kosten.
  - Privacy beleid opstellen
  - Processen uitschrijven
  - Procedures uitschrijven
  - Keuzes maken
  - IT aanpassen (Privacy by design)
  - IT aanpassen (beter beveiligen)
  - IT aanpassen rechten van de betrokkene etc etc

Conclusie

1. Botsing AVG en goed risicomanagement / prijsstelling
2. Er ontstaan risico's voor ondernemer: business-, privacy-, reputatie risico's
3. Verwacht onduidelijkheid in interpretatie: jurisprudentie nodig
4. Ga uit van uw eigen innerlijk kompas, maak beleid, leg keuzes vast en handel naar uw keuzes
5. Breng de vier contexten in evenwicht
6. AVG gaat geld en management attentie vragen
7. Het zal minimaal drie tot vijf jaar duren voordat de markt de implementatie van de AVG volledig heeft verwerkt