Gegevensbescherming/Privacy

Invoering AVG bij de SVB

Hatice Dogan
Functionaris Gegevensbescherming

17 mei 2018

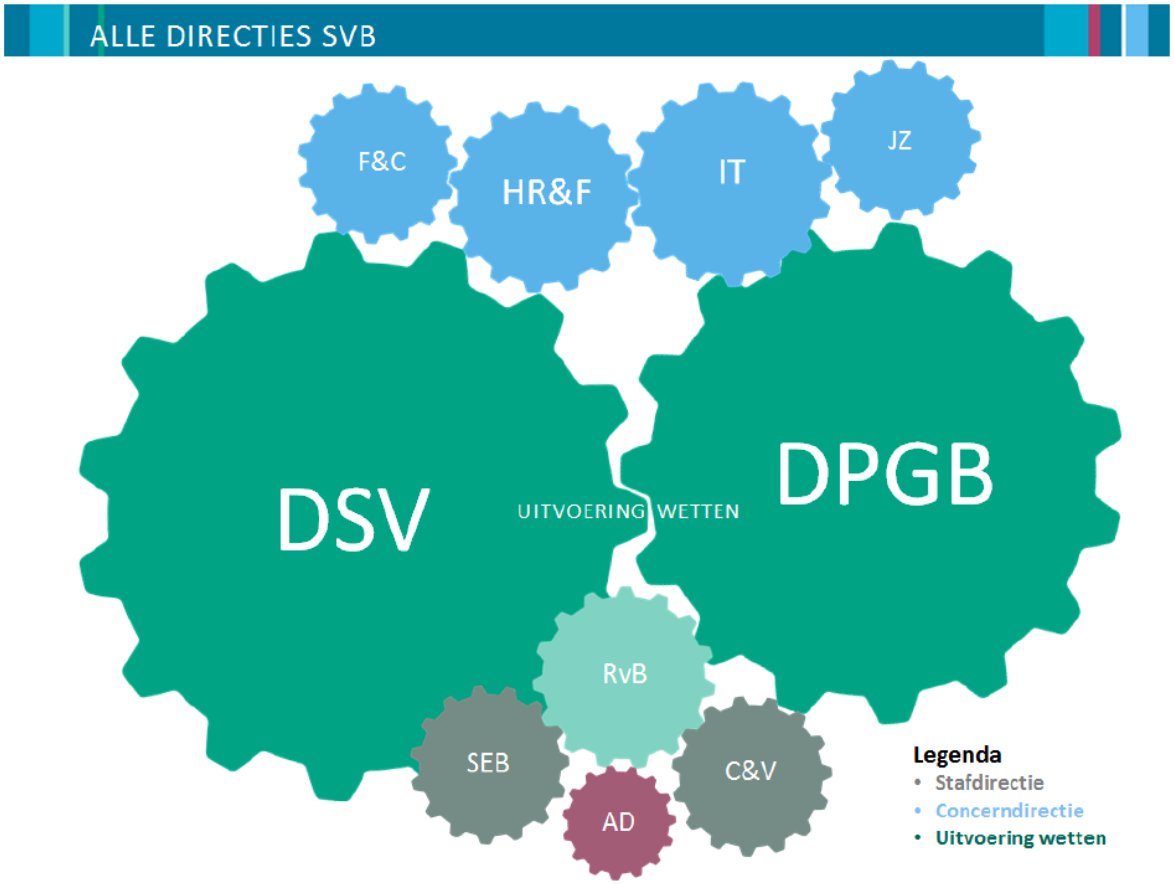
voor het leven
Sociale Verzekeringsbank

Wat nu!

- 'Veel bedrijven voldoen nog niet aan nieuwe Europese privacywetgeving'
- Veel Nederlandse bedrijven voldoen minder dan twee weken voor de deadline nog niet aan de nieuwe Europese privacyregels. Veelal is achterstallig onderhoud de reden dat de deadline niet gehaald gaat worden..
- Ondernemersverenigingen VNO-NCW en MKB Nederland erkennen dat zowel grote als kleine bedrijven minder dan twee weken voor de deadline nog niet klaar zijn voor de nieuwe wetgeving, mede omdat de huidige wet niet goed wordt nageleefd.
- Organisaties zijn vanaf 25 mei verplicht om precies te documenteren welke privégegevens van wie ze in bezit hebben, hoelang ze die bewaren en wat ze er mee doen. Ook hebben mensen meer mogelijkheden om data te laten verwijderen en is voor sommige ondernemingen een speciale privacyfunctionaris verplicht.
- Vanaf 25 mei kan de Autoriteit Persoonsgegevens bij een overtreding van de nieuwe wetgeving forse boetes uitdelen die kunnen oplopen tot miljoenen euro’s.

SVB is een grote dataverwerker

Figuur 1.2 Organigram SVB



S V B
voor het leven
Sociale Verzekeringsbank

SVB en gegevensbescherming

- SVB is een ‘data gedreven’ organisatie
- Kernactiviteiten van de SVB zijn gericht op de registratie en het gebruik van persoonsgegevens
- Gegevensbescherming van zeer groot belang
- Gegevensbescherming:
  - Gedrag
  - Informatiebeveiliging (CISO)

Belangrijkste beginselen gegevensbescherming

- Doelbinding
- Rechtmatige grondslag
- Kwaliteit
- Transparantie of openheid
- Beveiliging
- Rechten betrokkenen
- Buitenlands gegevensverkeer

WBP en de AVG

PERSOONSGEGEVENS

DAAR ZIJN WE ZUINIG OP

S V B

voor het leven
Sociale Verzekeringsbank

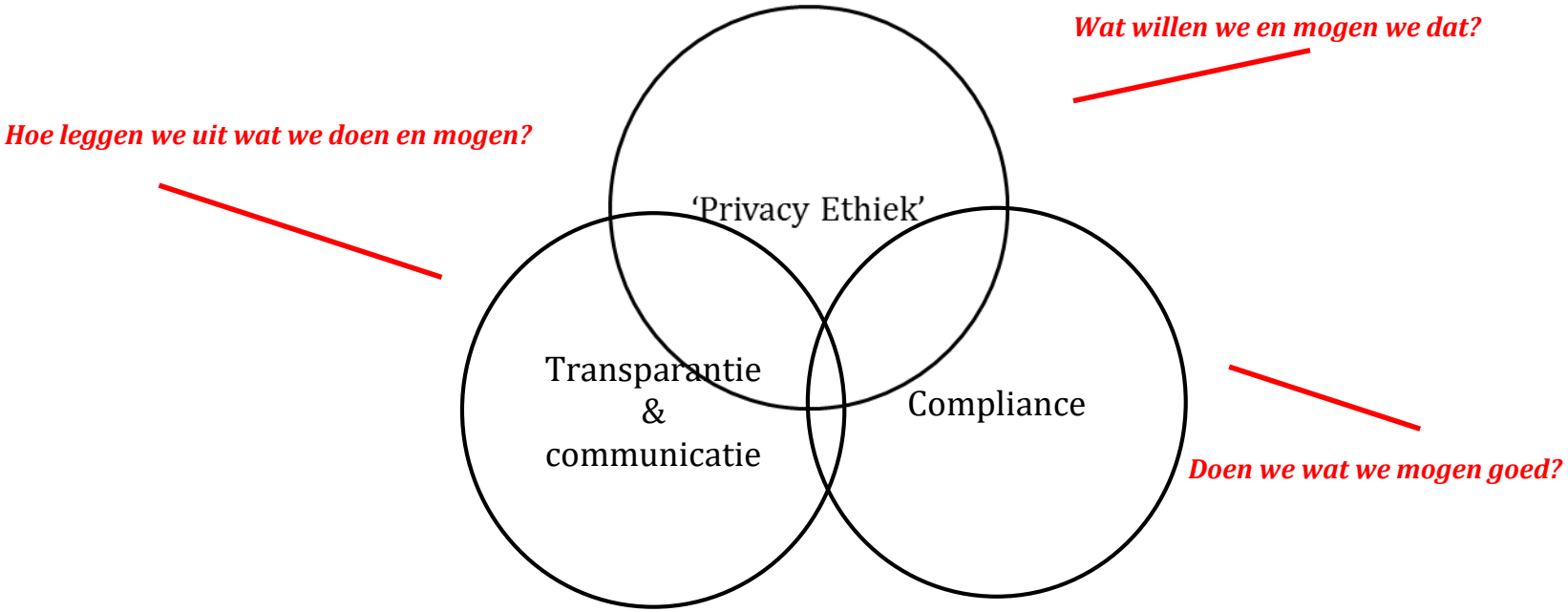
Bescherming persoonsgegevens

Wat is

Privacy Grondrecht

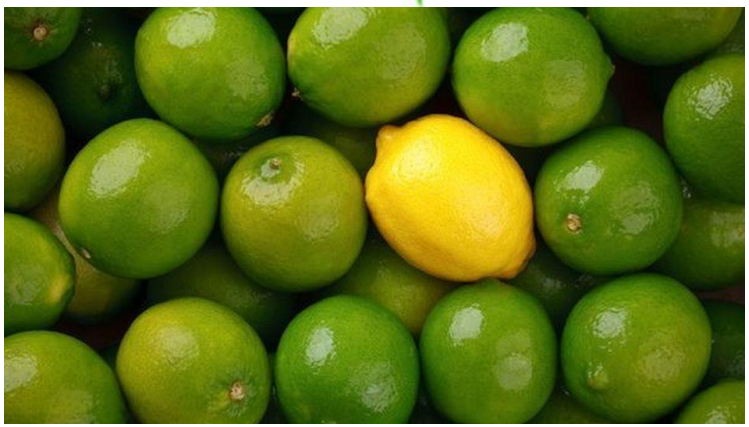
- Artikel 10 lid 2 Gw / artikel 8 EVRM
- Beperking bij wet

Aspecten van privacy & vertrouwen



Privacy is context

- Wie zijn de spelers
- Wat is het speelveld
- Wat zijn de spelregels



Spelers

de spelers

- Betrokkene
  - degene op wie de gegevens betrekking hebben
  - natuurlijke persoon
- Verwerkingsverantwoordelijke
  - heeft zeggenschap over doel en wijze van verwerking
  - natuurlijk persoon of rechtspersoon, of bestuursorgaan
- Verwerker

  -verwerkt gegevens t.b.v. verantwoordelijke zonder aan zijn of rechtstreeks gezag te zijn onderworpen
- Autoriteit Persoonsgegevens
- Functionaris Gegevensbescherming

Speelveld

het speelveld

- verwerking persoonsgegevens

  -persoonsgegevens zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon

  -verwerking is elke handeling(en) m.b.t. persoonsgegevens

- bestand
- persoonlijk of huishoudelijk
- journalistiek
- territoriale werking

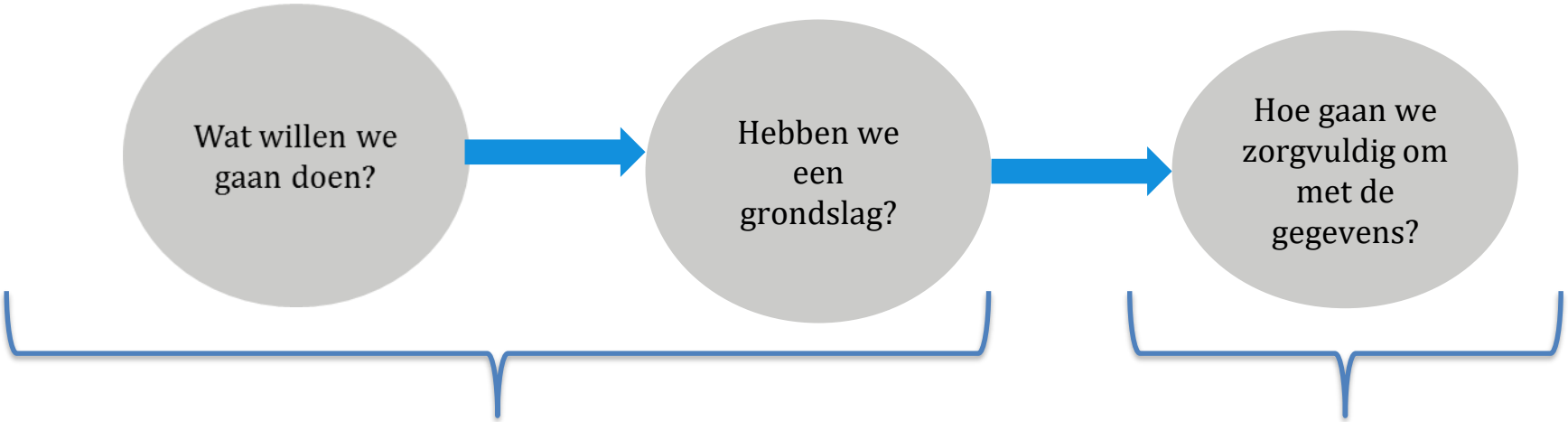
Spelregels

de spelregels

- verwerkingsgrondslag
- doelbinding
- bewaren
- beveiligen
- bijzondere persoonsgegevens en bsn
- enz.

Sociale Verzekeringsbank

Logica van de AVG



Logica van de Wbp/AVG

- Verwerk geen persoonsgegevens zonder duidelijk doel (art. 5 AVG)
- Zorg dat het doel gebaseerd is op een legitieme grondslag (art. 6 AVG)
- Gebruik de gegevens alleen voor dit doel of verenigbare doelen (art. 5 AVG)
- Verwerk geen bijzondere persoonsgegevens, tenzij…(art. 9 AVG)

Materiële eisen AVG

- Verzamel niet meer gegevens dan nodig (art. 5 AVG)
- Zorg dat de gegevens toereikend en correct zijn (art.5 AVG)
- Zorg dat de gegevens veilig zijn (art. 24 en 25 AVG Privacy by design and default)
- Bewaar de gegevens niet langer dan nodig (art. 5 AVG)
- Wees open en transparant (art. 30 AVG Registerplicht)

Privacy als risicofactor

- Baten en risico
- Reputatieschade
- Handhaving door de AP
- Meldplicht datalekken

Doel AVG

Belangrijkste punten

- grotere transparantie voor de burger (**informatieplicht**)
- verstevigde rechten van de burger en aangescherpte verplichtingen van de verantwoordelijken (**registerplicht**)
- Privacy by design and default (gegevensbescherming door ontwerp en door standaardinstellingen, denk aan dataminimalisatie, pseudonomisering, doel- en grondslagbepaling)
- PIA’s
- verscherping van het toezicht door de toezichthouder
- verplichting benoeming FG voor een overheids- of bestuursorgaan

Waar raakt privacy de organisatie?

- Gegevens klanten (ihkv wetsimplementatie)
- Pre- en inemployment screening
- HR beleid / loonadministratie
- Monitoring personeel
- Facturering
- Exploitatie website
- Afspraken met leveranciers en derden
- etc. etc.

Wie is verantwoordelijk voor het privacybeleid?

- De privacy officer / functionaris gegevensbescherming?
- De juridische afdeling?
- De ICT afdeling?
- Het management?
- Niemand?

Hoe kunnen we risico's ontdekken

- PIA/GEB
- Identificeren privacyrisico's binnen een beleid/product/project/dienst en deze te adresseren
- Draagvlak creëren en verantwoording afleggen over gemaakte keuzes
- Privacybescherming expliciet meenemen in het ontwerp (privacy by design)

Meldplicht datalekken

- Inbreuk in verband met persoonsgegevens
- Waarschijnlijk een risico voor de rechten en vrijheden van de betrokkenen
- Melden binnen 72 aan de AP
- Informeren betrokkenen

Wat gaat de SVB doen

- AVG is een generieke wet
- Nagaan welke verwerkingen er zijn
- Vaststellen of deze rechtmatig plaatsvinden. Dat betreft bijvoorbeeld de noodzaak, de kwaliteit en de doelbinding
- Meldingenregister realiseren
- De opgeslagen gegevens niet langer bewaren dan noodzakelijk is
- Passende beveiligingsmaatregelen treffen
- Informatie verstrekken aan de betrokkenen, en hun rechten, zoals het recht op inzage, correctie of verzet, op verzoek effectueren
- Periodiek nagaan of de melding dan wel de afspraken die zijn gemaakt nog steeds geldig zijn of moeten worden aangepast

voor het leven
Sociale Verzekeringsbank

Kader vastgesteld door CIP

Beleid

B.01 Privacybeleid
1.Privacy beleid
2.Invulling wet.beginselen

B.02 Org.inbed-ding
1.Taken & Verantw.
2.Benodigde middelen
3.Rapportering

B.03 Risk Man/ PbD/GEB
1.Beoordelen Risico's
2.Passende maatregelen
3.Aantonen

Uitvoering

U.01 Doelbinding
1.Tijdig, welbepaald, uitdrukkelijk
2.Doeleinden
3.Verdere verwerking
4.Bijzondere persoonsgegevens
5.Strafrechtelijke veroordelingen en strafbare feiten
6.Nationaal ID nr
7.Geautomatiseerde besluitvorming
8.Statisch onderzoek

U.02 Register
1.Register
2.Actueel & samenh. Beeld

U.03 Kwaliteitsmgt
1.Juistheid & nauwkeurigheid
2.Geïnformeerd

U.04 Info.beveili-ging.
1.Tech. & org. Maatr.
2.Passend niveau (BIR)

U.05 Informatie-plicht
1.Tijdig
2.Informatie
3.Toestemming
4.Uitzondering

U.06 Bewaren van pg's
1.Bewaartermijn
2.Maatregelen

U.07 Doorgifte pg's
1.Onderl. verantw.
2.Afd. garanties
3.Vertegenwoor-diger
4.Uitzonderings-grond
5.Adequaatheidsbesluit
6.Passende waarborgen
7.Afw. Specifieke situatie

Controle/ beheer

C.01 Intern toezicht
1.Evaluatie
2.Rechtmatigheid aangetoond

C.02 Inzagerecht
1.Informatie
2.Tijdig
3.Passende vorm
4.Specifieke uitzonderingsgrond
5.Correctierecht & overdraagbaarheid

C.03 Meldplicht datalekken
1.Melden
2.Tjidig
3.Documentatie
4.Uitzondering

Legenda

Domein

Norm

=Norm met directe uitwerking voor de burger

Maatregel

Conclusies

- Privacy is subjectief en sterk context gebonden
- Privacybescherming is een integraal onderdeel van ‘good governance’
- Privacywetgeving wordt steeds strenger (en boetes hoger!)
- Laat geen onduidelijkheid ontstaan over wie de verwerkingsverantwoordelijke is

Einde

Dank voor jullie aandacht

voor het leven
Sociale Verzekeringsbank