Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer

Organisatiebeheersing en informatieveiligheid

Caroline Vernaillen & Anne Teughels
21 maart 2013

Organisatiebeheersing en informatieveiligheid

INLEIDING

- **Wie** zijn wij
- **Waarom** informatieveiligheid
- **Hoe** past informatieveiligheid in organisatiebeheersing

Overheidscommunicatie en informatieveiligheid

WIE

- **Wie** zijn wij
  - adviseurs van de VTC
  - **De Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer**

Opgericht bij E-GOV decreet

Verantwoording aan Vlaams Parlement

Controleren van stromen van persoonsgegevens die uitgaan van een Vlaamse instantie

Hoe:1° machtigen van die stromen
2° adviezen (regelgeving, VDI-decreet)
3° beantwoorden van vragen en begeleiding

Organisatiebeheersing en informatieveiligheid

WAAROM

'De jongste maanden zagen we de fraudes bij onlinebankieren toenemen', zegt CEO Michel Vermaerke van Febelfin, de Belgische federatie van de financiële sector. *'Vaak gebruiken de fraudeurs persoonlijke informatie om het vertrouwen van de slachtoffers te winnen, en hen met een geloofwaardig verhaal te overtuigen om hun codes te openbaren. Met de virale video wilden we mensen duidelijk maken dat ze zulke informatie vaak zelf op het internet hebben achtergelaten. Soms zonder het zelf te beseffen.'*

https://www.youtube.com/watch?v=F7pYHN9iC9I

en enkele voorbeelden bij overheden …

http://www.computerweekly.com/news/2240084015/UK-government-loses-data-on-25-million-Britons

http://news.cnet.com/U.K.-government-loses-pensioner-data/2100-1029_3-6223493.html

http://webwereld.nl/nieuws/108815/weer-certificatenleverancier-overheid-gehackt.html

http://frontpage.fok.nl/nieuws/214628/1/1/50/franse-overheid-gehackt.html

Organisatiebeheersing en informatieveiligheid

WAAROM

“NMBS heeft een groter probleem dan het denkt

De gegevens van 1,5 miljoen NMBS-klanten zijn gelekt. En dat is een veel groter probleem dan wij denken.
Dat dit zomaar kon gebeuren is al bedroevend. Maar de manier waarop de NMBS met deze situatie omgaat is nóg bedroevender.

De NMBS ondernam via twitter weliswaar een minieme poging tot het aanbieden van verontschuldigingen, op zijn website is van enig excuus geen sprake. Integendeel, het spoorbedrijf gaat direct in de verdediging en minimaliseert het datalek. Het gaat om “een gedeelte” van het klantenbestand (anderhalf miljoen! anderhalf! miljoen!) dat maar “een heel korte tijd” beschikbaar zou zijn geweest (in werkelijkheid ging het om bijna een maand). Het zou bovendien enkel zichtbaar zijn voor wie “geavanceerde kennis heeft van zoekmachines”. Een geruststellende gedachte: je opa kon de gegevens niet raadplegen….”

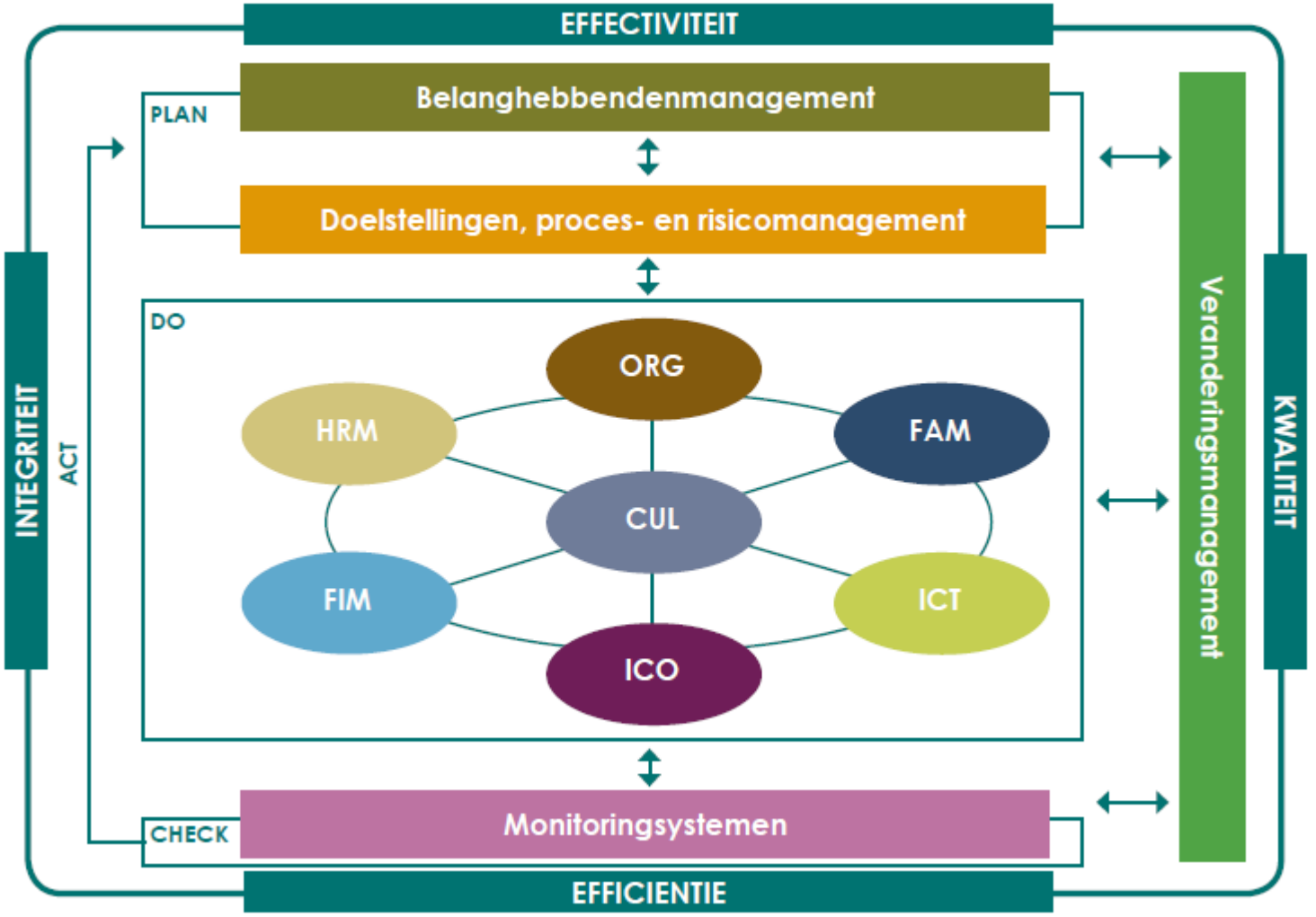
Bron: http://samfeys.be/nmbs-heeft-een-groter-probleem-dan-het-denkt/
Zie ook: http://datanews.knack.be/ict/nieuws/nmbs-lek-naar-justitie/article-4000229416512.htm

Organisatiebeheersing en informatieveiligheid

HOE

- **Hoe past informatieveiligheid in organisatiebeheersing ?**

Organisatiebeheersing en informatieveiligheid



Organisatiebeheersing en informatieveiligheid

Register online

Bescherming van persoonsgegevens geldt in meeste domeinen organisatiebeheersing

- HR: personeelsgegevens!
- Communicatie: klantengegevens, cookies, sociale media, …
- Facilitair: gebouwinfrastructuur, toegang, bewaking
- Cultuur: deontologie, awareness, sociale media
- ICT: natuurlijk

Organisatiebeheersing en informatieveiligheid

HOE

Bij de uitbouw of optimalisatie van de organisatiebeheersing moeten de volgende principes voor ogen gehouden worden:

- **Organisatiebeheersing is ingebouwd in de processen en loopt continu**.
- **Organisatiebeheersing is een zaak van iedereen**.
- **Organisatiebeheersing verschaft redelijke zekerheid**.

Organisatiebeheersing en informatieveiligheid

HOE

Bij de uitbouw of optimalisatie van de organisatiebeheersing moeten de volgende principes voor ogen gehouden worden:

- **Informatieveiligheid is ingebouwd in de processen en loopt continu**. Privacy by Design
- **Informatieveiligheid is een zaak van iedereen**.
- **Informatieveiligheid verschaft redelijke zekerheid**.

Organisatiebeheersing en informatieveiligheid

Organisatiebeheersing (of interne controle): redelijke zekerheid bekomen in de volgende domeinen:

- het bereiken van de opgelegde **doelstellingen** en het effectief en efficiënt beheer van **risico's**; ✓
- de naleving van **regelgeving en procedures**; ✓
- de betrouwbaarheid van de **financiële en beheersrapportering**; ✓
- de effectieve en efficiënte **werking** van de diensten en het efficiënt inzetten van de **middelen**;
- de bescherming van haar **activa** en de voorkoming van **fraude**. ✓

Organisatiebeheersing en informatieveiligheid

HOE

Volgen van reglementen en procedures

Voor Vlaamse overheidsinstanties gelden

- de privacywet
- het e-govdecreet

Risicobeheersing of informatieveiligheid sensu stricto

Organisatiebeheersing en informatieveiligheid

Volgen van reglementen en procedures

- **De privacywet**:

wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (WVP)

http://vtc.corve.be/wetgeving.php

Organisatiebeheersing en informatieveiligheid

- Definitie van **persoonsgegeven**:

iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon …

= zeer ruim
= niet beperkt tot privacy/persoonlijke levenssfeer

Organisatiebeheersing en informatieveiligheid

- Definitie van **verantwoordelijke voor de verwerking**

Niet de IT-dienst
Niet de personeelsleden
WEL het management – het hoofd van de entiteit

= verantwoordelijk voor de naleving van de privacywet

Organisatiebeheersing en informatieveiligheid

HOE

- **De principes** van de privacywet naleven:

Finaliteit

Proportionaliteit

Transparantie

Veiligheid

Organisatiebeheersing en informatieveiligheid

- **Het e-govdecreet**:

Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer
http://vtc.corve.be/docs/egov_decreet.pdf

Organisatiebeheersing en informatieveiligheid

- Artikel 6: verplichtingen Vlaamse Bestuursinstanties

§ 1. **De instanties zijn in ieder geval verplicht** :

1° persoonsgegevens te verwerken overeenkomstig de **privacywet**;

2° bij iedere nieuwe toepassing van het elektronische bestuurlijke gegevensverkeer vooraf adequate technische en organisatorische maatregelen in te bouwen voor de naleving van de **privacywet**;

3° op elk moment te waken over **de kwaliteit en de veiligheid** van gegevens en alle maatregelen te treffen om een perfecte bewaring van persoonsgegevens te garanderen;

4° de **toezichtcommissie te ondersteunen** bij de vervulling van haar opdrachten;

5° de **toezichtcommissie informatie** te verstrekken **en inzage** in alle dossiers en informatieverwerkende systemen te verschaffen telkens als ze daarom vraagt.

Organisatiebeheersing en informatieveiligheid

- Artikel 8: machtigingsverplichting

De **elektronische mededeling** van **persoonsgegevens** door een **instantie** vereist een machtiging van de Toezichtcommissie[...]

Organisatiebeheersing en informatieveiligheid

- Artikel 9: Veiligheidsconsulent

Iedere instantie die een authentieke gegevensbron beheert die persoonsgegevens bevat, **iedere instantie**
die elektronische persoonsgegevens ontvangt of uitwisselt, en iedere entiteit die overeenkomstig artikel 4, § 3, aangewezen is en persoonsgegevens verwerkt, wijst een **veiligheidsconsulent** aan. De Vlaamse Regering bepaalt de opdrachten en de manier van aanwijzing van die veiligheidsconsulenten.

http://vtc.corve.be/docs/E_GOV_decreet_BVR_VEILIGHEID.pdf
http://vtc.corve.be/docs/Aanvraag_advies_aanstelling_veiligheidsconsulent.doc

Organisatiebeheersing en informatieveiligheid

- Sancties:
  - niet naleven privacywet is strafbaar
  - verwerking/gegevensstroom kan worden stopgezet
  - tuchtsancties/ontslag

- Schadeclaims

- Vertrouwen in de Vlaamse Overheid krijgt een deuk

Organisatiebeheersing en informatieveiligheid

Informatieveiligheid - risicobeheersing

Leidraad Interne Controle Organisatiebeheersing:

10.1.6 Beveiligingsmanagement

ICT-beveiliging is het geheel van maatregelen (voorschriften, processen, activiteiten,…) dat ervoor zorgt dat informatiesystemen (bedrijfs- en bestuursprocessen) een optimale bescherming genieten (rekening houdend met het kosten-baten principe) op het vlak van vertrouwelijkheid, **privacy**, integriteit en beschikbaarheid.

Organisaties moeten hun ICT-veiligheidsbeleid uitstippelen vanuit **drie invalshoeken**: de menselijke factor (veiligheidscultuur), de processen en de technologie. Alleen op deze manier zal de integriteit, vertrouwelijkheid en beschikbaarheid van informatie immers gewaarborgd zijn.

Organisatiebeheersing en informatieveiligheid

Informatieveiligheid

- ook informatie op papier
- betreft niet alleen persoonsgegevens maar ook
  - andere vertrouwelijke informatie
  - de beschikbaarheid en betrouwbaarheid van de informatie voor beleid, voor dossierverwerking,…

Organisatiebeheersing en informatieveiligheid

HOE

Belangrijkste instrumenten:

- informatieveiligheidsconsulent
- informatieveiligheidsplan

Organisatiebeheersing en informatieveiligheid

- Informatieveiligheidsplan

- ISO 27002 norm als inspiratie (cf. IT-dienst)
- Richtsnoeren privacycommissie
  http://vtc.corve.be/infoveiligheid.php
- Leidraad Organisatiebeheersing (p. 86)
  http://www.bestuurszaken.be/sites/bz.vlaanderen.be/files/Leidraad%20interne%20controle.pdf

Organisatiebeheersing en informatieveiligheid

- Informatieveiligheidsplan
  - ! risico-analyse
  - ! awareness
  - ! voldoende middelen
  - ! stappenplan
  - ! contract met de verwerker (dataleverancier, (onder)aannemer)

Organisatiebeheersing en informatieveiligheid

- Informatieveiligheidsplan

  Hoofdstukken:

1. Risico
2. Beleid
3. Organisatie: intern + externe partijen
4. Bedrijfsmiddelen: classificatie informatie!
5. Personeel
6. Fysieke omgeving
7. Communicatie en operationele procedures
8. Toegang tot persoonsgegevens
9. Aanschaffen, ontwikkelen en onderhouden informatiesystemen
10. Informatiebeveiligingsincidenten
11. Bedrijfscontinuïteit
12. Naleving

Organisatiebeheersing en informatieveiligheid

- Recente aanbeveling privacycommissie ivm datalekken

  http://vtc.corve.be/docs/CBPL_gegevenslekken_aanbeveling_01_2013.pdf

- CLOUDproblematiek

Organisatiebeheersing en informatieveiligheid

BESLUIT

- **Besluit :** neem privacy en informatieveiligheid mee wanneer jullie plannen maken in de verschillende domeinen en integreer dit ook in de globale organisatiebeheersing

- Linken
  - www.vlaamsetoezichtcommissie.be
  - www.privacycommission.be

- Vragen? toezichtcommissie{at}vlaanderen{dot}be