28 januari 2021

Dag van de privacy

Informatiebeveiliging en Privacy - Corona Team

"Privacy gaat niet om wat je te verbergen hebt, maar om wat je te beschermen hebt"

~Edward Snowden

[redacted] – CISO/FG

Veiligheids- en Gezondheidsregio Gelderland-Midden

Privacy, Cyber en Informatiebeveiliging

Privacy

- Wetgeving
- Gaat alleen over persoonsgegevens
- Is een grondrecht
- Niet voldoen = risico op boete

Cyber

- Techniek
- Alle digitale gegevens
- Kans op directe schade voor de bedrijfsvoering

IB

- IT , HRM, gebouwbeheer, stroom, bedrijfscontinuïteit
- Beschikbaarheid, integriteit en vertrouwelijkheid van informatie
- Breed over de bedrijfsvoering heen.

Masterclass Informatiebeveiliging en Privacy

Doel

- Informeren over de vereisten inzake informatiebeveiliging en privacy;
- wat doen we bij VGGM;

… en meer specifiek, *wat moeten we doen binnen het corona-team?!*

Agenda

• AVG als wettelijk kader voor privacy	ca. 15 min
• Informatiebeveiliging (NEN7510)	ca. 10 min
• Meldplicht datalekkken	ca. 10 min
• Vragen en vervolg	ca. 5 min

Privacy (in context)… wat is dat eigenlijk?

Artikel 8 van het Europees Verdrag voor de Rechten van de Mens
‘.. Recht op eerbiediging van privé-, familie- en gezinsleven.. ‘

Artikel 10 Nederlandse Grondwet:
‘… het recht van iedereen om in de beslotenheid van zijn persoonlijke levenssfeer met rust te worden gelaten …

“De mogelijkheid om in je eigen omgeving jezelf te zijn.”

“het recht van het individu om in beginsel zelf te beschikken over de openbaarmaking en het gebruik van persoonlijke gegevens”

De Verordening

Algemene Verordening Gegevensbescherming

- Voor de bescherming van grondrechten en fundamentele vrijheden. Privacy!

Van Wbp naar AVG

- De AVG vervangt Wet bescherming persoonsgegevens (Wbp)

Hoe?

- Voor alle organisaties “in” Europa.
  Ook verenigingen en stichtingen.
- Passende maatregelen om (persoons)gegevens zorgvuldig en veilig te verwerken.
- Rechten voor betrokkenen.
- Meer bevoegdheden voor toezichthouders.

Verwerken van persoonsgegevens

Verwerken:

- alle handelingen die een organisatie kan uitvoeren met persoonsgegevens; van verzamelen tot en met het vernietigen.

  *Verzamelen, vastleggen of opslaan, bijwerken of wijzigen, gebruiken, opvragen of **raadplegen**, verspreiden of versturen, beschikbaar stellen, wissen en vernietigen van gegevens.*

Persoonsgegevens

- (Gevoelige) persoonsgegevens
- Bijzondere persoonsgegevens

  o.a. Gezondheid, ras en etniciteit, godsdienst, politieke opvattingen, seksuele voorkeur…

Doel en grondslag zijn noodzakelijk

Gegevens enkel verwerken met doel en een van de zes grondslagen.

Op basis hiervan mag je persoonsgegevens verzamelen

De grondslag

Toestemming van de gebruiker

Vitale belangen

Wettelijke verplichting

Overeenkomst

Algemeen belang

Gerechtvaardigd belang

Veiligheids- en Gezondheidsregio Gelderland-Midden

De theorie samengevat:

Breng in kaart welke persoonsgegevens je verwerkt en ga na of alle gegevens wel echt nodig zijn en welk maatregelen je neemt (Evt. met behulp van een DPIA.)

Zorg voor informatiebeveiliging met passende technische en organisatorische maatregelen.

Sluit verwerkersovereenkomst met partij (verwerker) als ze persoonsgegevens voor je verwerken.

Publiceer een privacyverklaring zodat voor iedereen duidelijk is wat je met persoonsgegevens doet.

Datalek altijd vastleggen en indien nodig, melden bij AP en bij betrokkene!

Geef gehoor aan Rechten van betrokkene.

AVG - Administratieve Verplichtingen geldt altijd

- Verwerkingsregister
  - De naam en contactgegevens van (de vertegenwoordiger van) jouw organisatie;
  - De doelen en grondslag waarvoor je de persoonsgegevens verwerkt;
  - Hoe de persoonsgegeven zijn verkregen;
  - Een beschrijving van de categorieën van personen van wie jij gegevens verwerkt;
  - Hoe lang je de gegevens bewaart;
  - De categorieën van ontvangers aan wie je persoonsgegevens verstrekt;
  - Een algemene beschrijving van de beveiligingsmaatregelen.
- Verwerkersovereenkomst
- Overzicht van datalekken en meldingen aan AP
- Privacyverklaring
- Uitvoeren DPIA (data protection impact assessment)

Rechten van betrokkene

- Het recht op informatie
- Het recht op inzage
- Het recht op rectificatie
- Het recht op dataportabiliteit
- Het recht op beperking van de verwerking
- Het recht op een menselijke blik bij besluiten
- Het recht van bezwaar
- Het recht op gegevenswissing (vergetelheid)

Organiseer het proces binnen het team!

Informatiebeveiliging wat is het?

Informatiebeveiliging is

- Het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen
- die de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie binnen een organisatie garanderen,
- met als doel de continuïteit van de informatie en informatievoorziening te waarborgen
- en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

Informatiebeveiliging (en overwegingen om het op te pakken)

Het gaat over:

- ❑ Data veiligheid
- ❑ Voldoen aan wet- en regelgeving (AVG, NEN7510)
- ❑ Bewustzijn van medewerkers
- ❑ Beschikbaarheid van de data/gegevens
- ❑ Zijn de gegevens juist (en blijven ze dat)
- ❑ Heeft *iedereen* toegang tot de gegevens (maar niet zomaar)

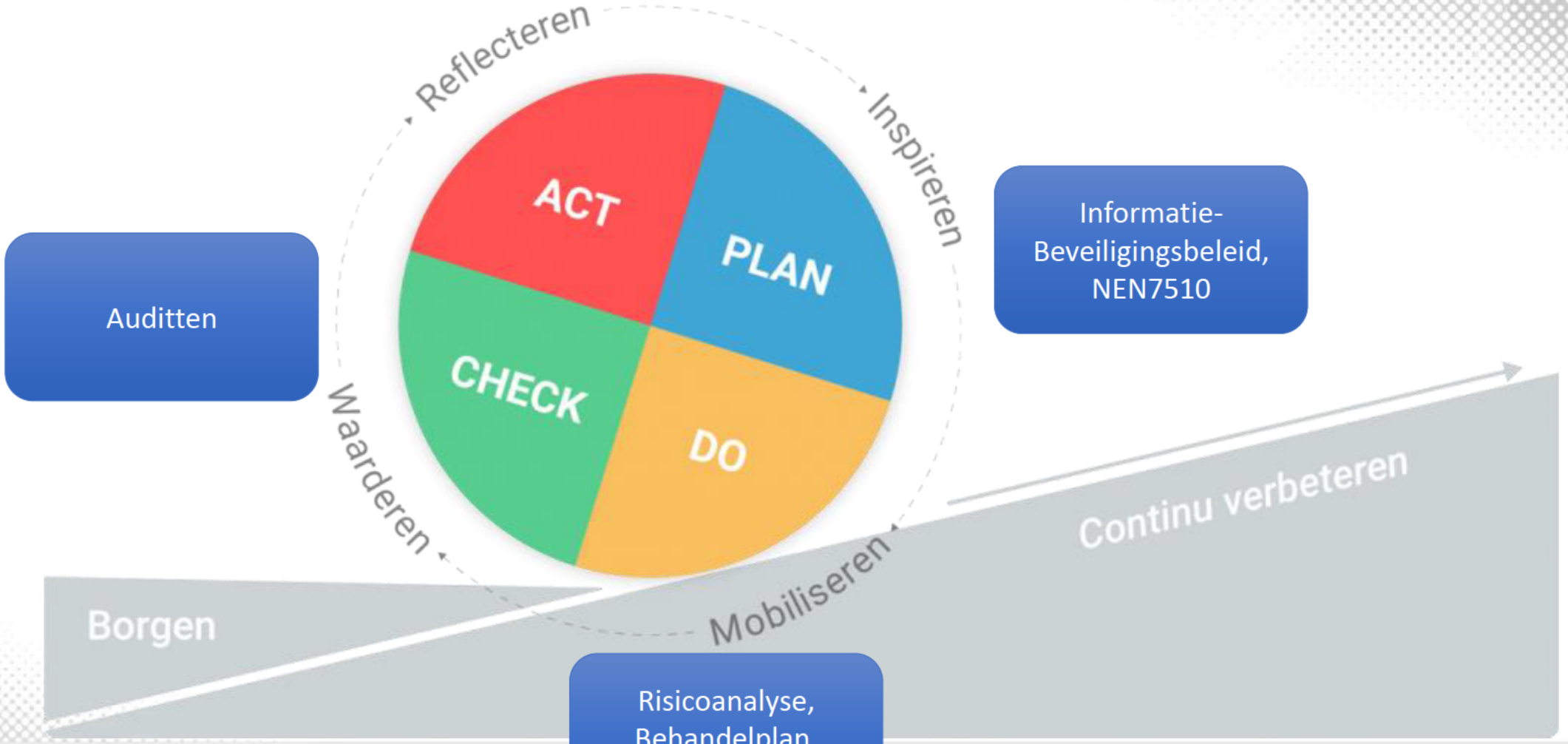
En ook over:

- ❑ Maatschappelijke verantwoordelijkheid nemen
- ❑ Verbetering en continuïteit van interne bedrijfsprocessen
- ❑ Formaliseren van beleid, richtlijnen en procedures

Veiligheids- en Gezondheidsregio Gelderland-Midden

ISMS

Managementreview



Auditten

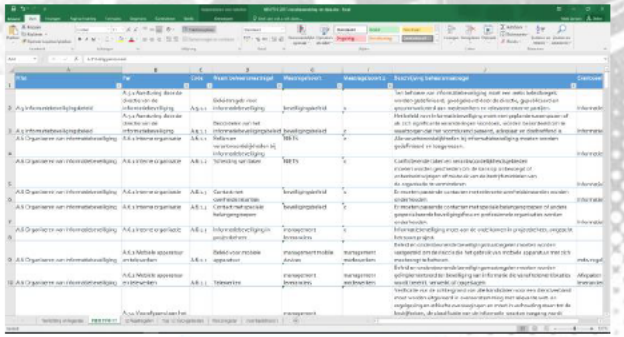
Informatie-Beveiligingsbeleid, NEN7510

Risicoanalyse, Behandelplan, IB-plan

Veiligheids- en Gezondheidsregio Gelderland-Midden

VGGM: voldoen aan BIO en NEN7510!

Hoofd stuk	Onderwerp
5	Informatiebeveiligingsbeleid
6	Organiseren en managen van Informatiebeveiliging
7	Veilig personeel (in- en uitdienst)
8	Beheer van bedrijfsmiddelen. Inventariseren, classificeren van data en media
9	Toegangsbeveiliging. Autorisatiematrices, wachtwoordenbeleid, inlogprocedures
10	Cryptografie
11.1	Fysieke beveiliging en beveiliging van de omgeving. Bescherming van kantoren en ruimtes
11.2	Apparatuur. Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.
12	Beveiliging van de bedrijfsvoering. Wijzigingenbeheer, inrichten OTA straat. Anti-Virus/Backup/monitoring en logging/kwetsbaarheden.



Hoofd stuk	Onderwerp
13	Communicatiebeveiliging. Netwerkbeveiliging, elektronische berichtentransport
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen
15	Leveranciersrelaties. Monitoren en beoordelen IB bij leveranciers.
16	Beheer van Informatiserings incidenten
17	Informatiebeveiliging continuiteit
18	Naleving en beoordeling. Controle op wettelijke vereisten, en rechten zoals Privacyrecht. Beoordeling rondom de naleving van de eisen

NEN

Veiligheids- en Gezondheidsregio Gelderland-Midden

Technische en organisatorische beveiligingsmaatregelen (NEN-7510/BIO)

- naar stand van de techniek

- Gedragscode
- Geheimhoudingsverklaring
- Opleiding en bewustwording
- (Werk) instructies!!
- Sluitend gebruikersbeheer
- Persoonlijke accounts en gebruik 2FA
- Logging (en controle hierop!)
- Privacy by default/privacy by design
- Beperken functionaliteiten
- Dataminimalisatie
- Encryptie (o.a. Zivver)

Meldplicht datalekken

Wat is een datalek ?

Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Zowel bij

- geautomatiseerd verwerkte persoonsgegevens;

- persoonsgegevens die op papier staan.

Ook wanneer persoonsgegevens per ongeluk worden vernietigd kan dit betekenen dat er sprake is van een datalek.

Vermoeden van datalek altijd direct melden bij de Servicedesk of leidinggevende!

Wat doet de Functionaris Gegevensbescherming met een melding van een datalek?

Tot nu:
7 datalekken,
2 gemeld + 1
via GGDGHOR

1. Beoordeelt of er sprake is van een datalek.
2. Beoordeelt of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens. (bij twijfel voorlopig melden, evt. intrekken)
3. Beoordeelt of de betrokken geïnformeerd moet worden.
4. Informeert *verantwoordelijken* in de organisatie.
5. Meldt het datalek bij de Autoriteit Persoonsgegevens.

   Let op: dit moet binnen 72 uur na bekend worden van het lek!
6. Adviseren over beperken van de impact en structurele verbeteringen.
7. Leren van incidenten

Ten onrechte niet melden kan leiden tot boetes!

AUTORITEIT
PERSOONSGEGEVENS

Veiligheids- en Gezondheidsregio Gelderland-Midden

Voorkom datalekken

Simpele maatregelen om datalekken te voorkomen

- Laat geen documenten liggen op de printer
- Kies een sterk wachtwoord (en houd het geheim)
- Gebruik geen USB-sticks van vreemden
- Klik niet op verdachte links in berichten
- Gebruik Zivver voor het versturen van bestanden
- Laat gegevens niet onbeheerd achter *(Clean desk, clear screen)*
- Vergrendel je computer als je je werkplek verlaat!
- Voorkom gebruik van openbare wifi-netwerken
- Voorkom oneigenlijk gebruik van gegevens, zoals inzien of kopiëren uit applicaties als HP zone, CoronIt, Osiris, email.
- Maak geen beeldmateriaal in je werkomgeving
- Wees alert op phishing!

Vragen

Zie ook het Intranet!