Vragen of tips tijdens de presentatie?
Reageer in de chat!

Privacy/AVG en Informatiebeveiliging - Bron & Contact Onderzoek

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

~Edward Snowden

– CISO/FG

Veiligheids- en Gezondheidsregio Gelderland-Midden

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.
- Passende maatregelen om (persoons)gegevens **zorgvuldig en veilig** te verwerken. **Plichten**.
- **Rechten** voor betrokkenen.

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”

Vragen of tips tijdens de presentatie?
Reageer in de chat!

Doel, noodzaak en rechtmatigheid

Gegevens verwerken met <u>doel, noodzaak,</u> en <u>rechtmatig</u>.

BCO: (Art.6 lid 1 sub e AVG en Lidstatelijk geregeld in artikel 6 lid 1 sub c Wet publieke gezondheid).

Op basis hiervan mag je persoonsgegevens verzamelen
De grondslag

Verwerken van persoonsgegevens in je dagelijks werk

Verwerken (art.4 lid 2 AVG)

- 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 (art.4 lid 1 AVG)

- Gewone persoonsgegevens (art.4 lid 1 AVG)
- Bijzondere persoonsgegevens (art.9 lid 1 AVG)

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

Ook bij BCO kan dit per situatie verschillen.

Vragen of tips tijdens de presentatie?
Reageer in de chat!

Rechten van betrokkene (Art.13 -20 AVG)

Het recht op informatie

Het recht op inzage

Het recht op gegevenswissing (vergetelheid)

Het recht op rectificatie

Het recht op dataportabiliteit

Het recht op beperking van de verwerking

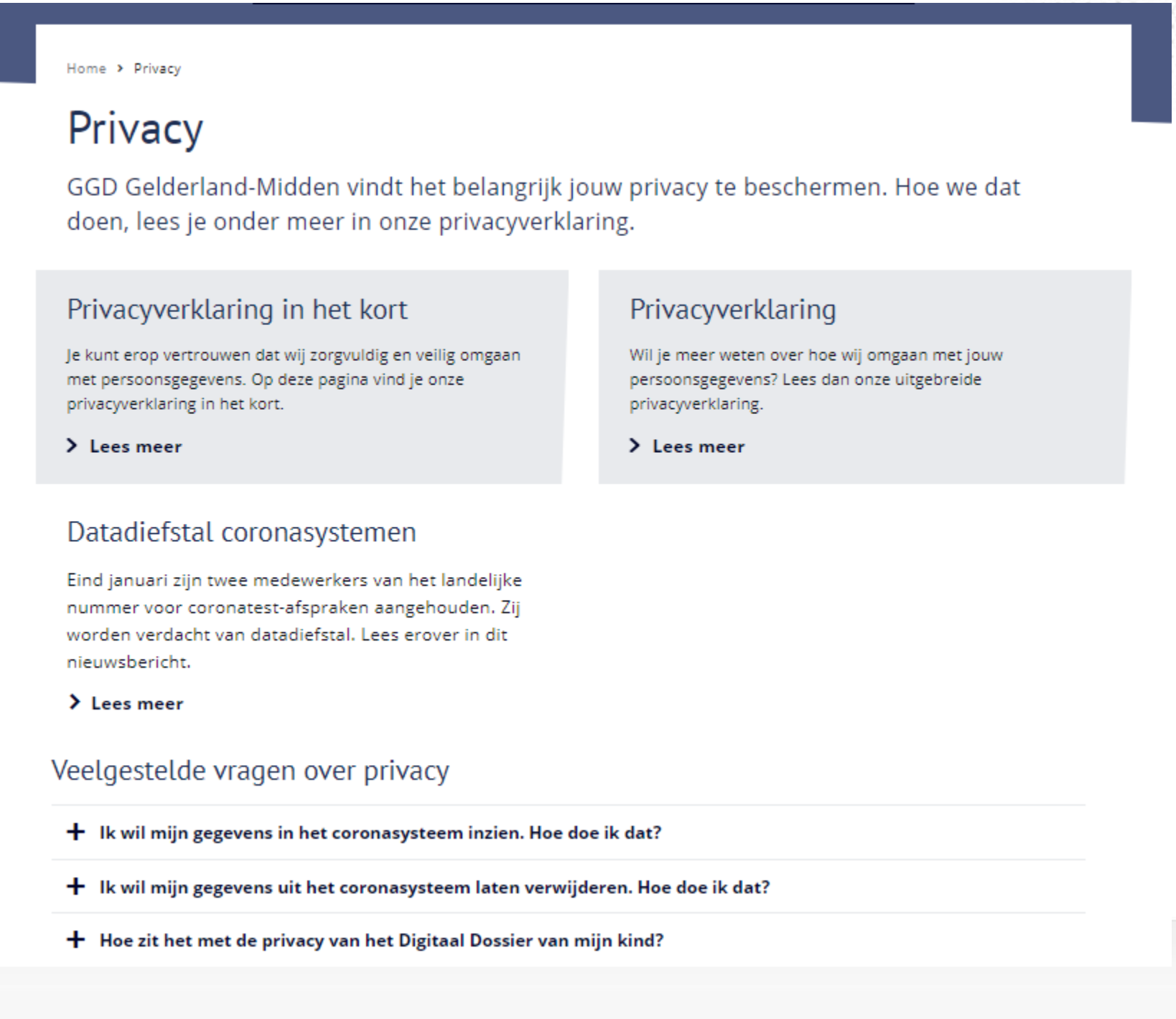
Het recht op een menselijke blik bij besluiten

Het recht van bezwaar

In de praktijk:

Na de datadiefstal bijzonder veel bezorgde burgers. Dit resulteerde in veel inzage- en verwijderverzoeken en verzoeken om informatie.

Context: Per situatie beoordelen.



Transparantie

Het recht op informatie

Via de privacyverklaring op internet

Recht op inzage en

Recht op gegevenswissing (vergetelheid)

Via de privacypagina op internet

Veiligheids- en Gezondheidsregio Gelderland-Midden

Zorgvuldig en (be)veilig(d)

Technische en organisatorische beveiligingsmaatregelen
- naar stand van de techniek (art.32 lid 1 AVG)

Norm:
NEN-7510 en BIO (Baseline informatiebeveiliging Overheid)

Randvoorwaarde om je werk te doen

- Gedragscode en Geheimhoudingsverklaring
- Geheimhoudingsplicht
- Opleiding en bewustwording
- Autorisaties en gebruikersbeheer (Privacy by default)
- Persoonlijke accounts en gebruik 2FA
- Logging (en controle hierop)
- Applicatie ontwikkeling (Privacy by design)

Vastleggen van informatie

BCO: noodzakelijke informatie conform instructie
Gegevens worden max. 5 jaar bewaard

Informatiedelen

<u>Met derden:</u>

- Indien dit volgens de wet moet (RIVM).
- Anders enkel met toestemming en alleen delen wat noodzakelijk is.

(Indien geen toestemming, dan geen negatieve gevolgen)

Gebruik veilige email (Zivver)

- (Werk) instructies → Landelijk/regionaal
- Opschonen van documenten, inbox, aantekeningen!

De 10 GOUDEN privacyregels

1 Alle informatie is vertrouwelijk

Informatie over de inhoud van je werkzaamheden, procedures en persoonsgegevens moeten geheim worden gehouden. Dit betekent dat je hierover bijvoorbeeld niets mag vertellen en schrijven, maar ook niets mag fotograferen. Zo houden we onze informatie veilig. Hiervoor heb je een geheimhoudingsverklaring ondertekend.

2 Volg de richtlijnen en werkinstructies

In de werkinstructies is opgenomen om welke gegevens mag worden gevraagd. Vraag niet om meer gegevens. Dubbelcheck daarnaast altijd de gegevens, zodat deze zeker goed in het systeem staan.

3 Bekijk alleen gegevens voor je werkzaamheden

Kijk niet naar gegevens van familie, vrienden of bekenden, tenzij een dossier specifiek aan jou is toegewezen. Er wordt door GGD GHOR Nederland actief gemonitord op onrechtmatige inzage van dossiers.

4 Houd wachtwoorden en toegangscodes voor jezelf

Houd je wachtwoorden voor jezelf en zorg dat niemand deze kan zien. Dit voorkomt onbevoegde inzage.

5 Gebruik Social Media verantwoord

- → Doe geen uitingen namens de GGD: het moet overduidelijk zijn dat het gaat om een privé post/mening.
- → Neem geen contact op met burgers vanuit privé hoedanigheid.
- → Laat je niet negatief uit tijdens én na beëindiging van je contract.

6 Meld datalekken altijd, zelfs bij alleen een vermoeden

Heb je een vermoeden van een datalek? Meld dit dan altijd volgens de procedure. Voorbeelden hiervan zijn:

- × Mail naar verkeerd e-mailadres
- × Geadresseerden in CC ipv BCC
- × Delen screenshot met persoonsgegevens
- × Verlies van laptop

7 Maak geen prints, screenshots of exports van gegevens

Bewaar persoonsgegevens van burgers alleen in de daarvoor bestemde veilige systemen en dus nooit op je pc, telefoon of op papier.

8 Houd je aan de Gedragscode thuiswerken: Clean desk en Clean screen

Zorg voor een goede werkplek met veilig internet, afgezonderd van anderen. Ga verantwoordelijk om met je apparatuur. En laat je scherm nooit openstaan.

9 Meld zaken die niet goed gaan

Wanneer je zaken in het proces ziet die niet goed lopen, neem dan contact op met je leidinggevende of de daarvoor bestemde contactpersoon, zodat actie kan worden ondernomen.

10 Stel vragen bij twijfel

Neem contact op met jouw leidinggevende als je twijfels hebt over de juiste uitvoering van jouw taak. Het voorkomen van onrechtmatige verwerkingen is voor ons en de burger dan beter te herstellen.

Vragen of tips tijdens de presentatie?
Reageer in de chat!

Meldplicht datalekken (art. 33 AVG)

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!

Vragen

- Waarom mogen we de voornaam van mensen niet noemen in de mail, maar wel de voorletter en de achternaam?
- Wat kunnen we doen om de informatie persoonlijker te maken met behoud van de AVG-richtlijnen?
- Mag je als GGD zijnde (of als arts) de huisarts en/of werkgever toch op de hoogte brengen, of mag je zijn huisgenoten op de hoogte brengen indien iemand niet wilt meewerken?
- Welke situaties zijn er allemaal waarbij de AVG (of de privacy van personen) minder zwaar weegt dan onze verplichtingen. Ik kan zelf twee situaties bedenken: Kindermisbruik en Zelfmoorddreiging. Maar zijn er nog andere situaties waarin ons beroepsgeheim wordt overruled?

Vragen

- Is er een DPIA gedaan voor het nieuwe systeem dat op dit moment gebouwd wordt? (GGD Contact)
- Wat doen wij er specifiek aan om de medewerkers te trainen en scherp te houden op het gebied van Data Privacy. (hoe vaak legen mensen hun mailbox (verzonden items etc)/bewaarde word documenten/gooien papieren op veilige manier weg)?
- Hoe brengen wij indexen en contacten op de hoogte van het feit dat wij persoonlijke data bewaren in het systeem – hoe lang bewaren we het – waar moeten ze zijn als zij hun dossier willen opvragen – hoe werkt dat – hoe vaak wordt dat in de praktijk gedaan?

Nog tijd voor vragen

Ook te stellen via chat of email

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
- Voorkom oneigenlijk gebruik van gegevens, zoals inzien of kopiëren uit applicaties als HP zone, CoronIt, Osiris, email.
- 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
- Maak geen beeldmateriaal in je werkomgeving
- Wees alert op phishing!

Wat kun jij doen om datalekken te voorkomen?

- Voorkom oneigenlijk gebruik van gegevens, zoals inzien of kopiëren uit applicaties zoals HP zone, CoronIT, Osiris, email.
  - → Dit kan leiden tot disciplinaire maatregelen.
  - → Ook het maken van beeldmateriaal in de werkomgeving is niet toegestaan!

- Verstuur zorggegevens altijd met beveiligde e-mail (Zivver)
  - → Vermijd het gebruik van Google Drive, Dropbox, WeTransfer etc.

- Voorkom gebruik van je werklaptop/werktelefoon voor privé doeleinden zoals social media, online shoppen, films streamen.
  - → Dit is not done, beperk dit en gebruik hiervoor zoveel mogelijk je privé device.

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

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. Laat organsiatie leren van incidenten.

Ten onrechte niet melden kan leiden tot boetes!

AUTORITEIT PERSOONSGEGEVENS

Veiligheids- en Gezondheidsregio Gelderland-Midden

Vragen