Werkinstructie Privacy

24 december2021

Inhoud

1. Aanleiding
2. Wettelijk kader
3. Privacy rechten
    a. Vereisten privacy rechten
    b. Recht op inzage
    c. Recht op correctie
    d. Recht op verwijdering
    e. Overige privacy rechten
4. Rol Privacy-Contactpersoon
5. Rol Compliance Officer
6. Datalekken
7. Bewaartermijnen
8. Documentatie
9. Privacy beleid GGD
10. FAQ privacy & BCO
11. Bijlagen
    a. Modelbrief ontvangstbevestiging verzoek

---

1. Aanleiding

Medewerkers hebben steeds vaker vragen hoe zij de privacy van cliënten kunnen borgen. Ook wordt door cliënten gevraagd om gegevens van hen in te zien, te verwijderen of te corrigeren. In deze FAQ/werkinstructie worden de belangrijkste privacy vragen beantwoord. De werkinstructie is een groeidocument en wordt steeds aangepast aan de hand van de laatste ontwikkelingen.

2. Wettelijk kader

Op bron- en contactonderzoek is de Wet publieke gezondheid van toepassing. Privacy vragen en verzoeken van cliënten over uitoefening van hun privacy rechten worden behandeld aan de hand van de Wet publieke gezondheid, de Algemene Verordening Gegevensbescherming en onderliggende wet- en regelgeving.

Op Testen en Vaccineren is de Wet op geneeskundige Behandelingsovereenkomst van toepassing. Privacy vragen en verzoeken van cliënten over uitoefening van hun privacy rechten worden behandeld aan de hand van de Wet geneeskundige behandelingsovereenkomst van toepassing, de Algemene Verordening Gegevensbescherming en onderliggende wet- en regelgeving.

Voor de praktische uitvoering van het BCO is door GGD GHOR de werkinstructie *'Bron- en Contact Onderzoek COVID-19. Werkinstructie Fase 1B: Volledig BCO zonder monitoring*[1]*'* (hierna: Werkinstructie GGD GHOR) opgesteld. Die werkinstructie is binnen de wettelijke kaders van de Wet publieke gezondheid het

[1] Let op: deze werkinstructie ziet enkel op Fase 1. Indien een andere fase van toepassing is, wordt de daarbij behorende werkinstructie gebruikt.

CONCEPT

uitgangspunt voor het handelen bij het BCO. De werkinstructie Privacy & BCO is een aanvulling op de Werkinstructie GGD GHOR en geeft antwoord op de (juridische) vragen die in de Werkinstructie GGD GHOR onbeantwoord blijven.

3. Privacy rechten

Verzoeken om inzage, correctie of verwijdering van gegevens moeten schriftelijk (dit kan ook per email) worden gedaan. Voordat een inzageverzoek op grond van de AVG in behandeling wordt genomen moet altijd eerst de identiteit worden vastgesteld van de cliënt.

a. Vereisten privacy rechten

- Binnen een maand na ontvangst van een verzoek moet een besluit zijn genomen over het verzoek. Een besluit op een verzoek op grond van de AVG is een besluit waartegen de cliënt een beroep kan instellen. Gebruik voor de reactie het 'Modelbesluit verzoek inzage gegevens (onder 5b).

- Cliënten dienen verzoeken in te dienen bij het Loket persoonsgegevens. Mocht een verzoek via een andere weg worden ingediend, verwijs de burger dan door naar het Loket persoonsgegevens. Hier is een standaard bericht voor (zie bijlage).

b. Recht op inzage

- Op grond van de AVG hebben cliënten van de GGD het recht om te vragen of zijn of haar persoonsgegevens worden verwerkt. Met dit recht op inzage kan een cliënt controleren welke persoonsgegevens door de GGD worden verwerkt en of deze persoonsgegevens wel kloppen. De GGD moet de cliënt op zijn of haar verzoek ook informeren over het gebruik van de gegevens: voor welke doeleinden worden de gegevens verwerkt, aan wie ze worden verstrekt en hoe lang ze worden bewaard.

- Naar aanleiding van een inzageverzoek verstrekt de GGD een overzicht waarin wordt aangegeven welke persoonsgegevens van een betrokkene worden verwerkt. Naast de persoonsgegevens zelf, moet de GGD bij een inzageverzoek de aanvullende informatie geven over de verwerking van zijn/haar persoonsgegevens door de GGD:
  a. waarom de persoonsgegevens door de GGD worden verwerkt;
  b. welke soorten persoonsgegevens de GGD verwerkt;
  c. indien van toepassing: aan welke organisaties de GGD persoonsgegevens doorgeeft. Dit geldt ook voor gegevens die de GGD doorgeeft aan organisaties in andere landen of aan internationale organisaties;
  d. hoe lang de GGD persoonsgegevens bewaart. Als de GGD dit niet precies kan aangeven, moet de GGD duidelijk kunnen maken welke criteria worden gehanteerd om een bewaartermijn te bepalen;
  e. welke privacyrechten betrokkenen hebben: het recht om hun persoonsgegevens te laten wijzigen, aanvullen of wissen, om te vragen om minder persoonsgegevens te verwerken en om bezwaar te maken als hun persoonsgegevens worden verwerkt;
  f. dat betrokkenen het recht hebben om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
  g. indien van toepassing: van welke organisatie de GGD persoonsgegevens heeft ontvangen als

CONCEPT

deze niet zelf zijn verzameld bij de betrokkene.

- Binnen een maand na ontvangst van het inzageverzoek moet een besluit zijn genomen over het geven van inzage.

c. Recht op correctie/aanvulling

- Een cliënt van de GGD kan vragen om correctie van zijn of haar gegevens indien: de gegevens feitelijk onjuist zijn (bijv. een naam, adres of telefoonnummer is verkeerd genoteerd), de gegevens niet compleet zijn, de gegevens niet relevant zijn voor het BCO of dat de gegevens op een andere manier gebruikt worden in strijd met een wet.

- Een cliënt kan geen correctie van zijn of haar gegevens vragen als hij of zij het oneens is met een uitslag, professionele indruk, mening of conclusie van de GGD. De cliënt kan de GGD wel vragen om een eigen verklaring aan de stukken toe te voegen.

d. Recht op verwijdering

- Een cliënt kan aan de GGD vragen om zijn of haar gegevens te verwijderen. Er moet in dat geval worden beoordeeld of de gegevens van cliënt verwijderd mogen worden. Binnen een maand na ontvangst van het verzoek om verwijdering moet een besluit zijn genomen.

e. Overige privacy rechten

- Naast het recht op inzage, correctie en verwijdering heeft een cliënt ook het recht op bijvoorbeeld een beperking van het gebruik van zijn of haar gegevens, bezwaar en gegevens over te dragen. Deze rechten zullen in praktijk minder worden ingeroepen en worden daarom niet in deze werkinstructie behandeld.

4. Rol Privacy Contactpersoon

Privacy Contactpersonen zijn het eerste aanspreekpunt voor medewerkers met betrekking tot privacy vragen. Daarnaast houdt de Privacy Contactpersoon toezicht in het geval van mogelijke problemen en datalekken. Als de Privacy-Contactpersoon vragen heeft die hij/zij niet zelf kan beantwoorden kan de hulp van de Privacy Officer [redacted]) worden ingeschakeld.

5. Rol Compliance Officer

Een Compliance Officer heeft de bevoegdheid om items/dossiers te kunnen muteren en te verwijderen. In deze rol zal de Compliance Officer de Privacy-Contactpersoon bijstaan in het afhandelen van correctie- en verwijderverzoeken.

6. Datalekken

Datalekken die waarschijnlijk een risico opleveren voor de cliënt, moeten binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens (AP). De desbetreffende medewerker die een datalek constateert meldt een datalek aan bij TOPdesk. De Privacy Contactpersoon pakt het datalek vervolgens direct op die via TOPdesk binnenkomen. Om binnen de termijn van 72 uur te blijven is het daarom belangrijk dat incidenten direct worden gemeld in TOPdesk. In het algemeen spreken we van een risico als een grote hoeveelheid persoonsgegevens zijn gelekt (kwantitatief ernstig) of als er gevoelige gegevens zijn gelekt (kwalitatief

CONCEPT

ernstig). Gevoelige persoonsgegevens zijn:Bijzondere persoonsgegevens (artikel 9 AVG);

- Gegevens over de financiële of economische situatie van de betrokkene(n);
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting van betrokkene(n);
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude, zoals inloggegevens en BSN.

Als een datalek is gemeld aan de AP dient tevens vastgesteld te worden of het datalek moet worden gemeld aan betrokkene(n). Hiervoor dient een aparte afweging gemaakt te worden. De Privacy Officer is verantwoordelijk voor het deze afweging.

Een datalek melden gaat als volgt:
Stap 1. Ga naar het Intranet van GGD Amsterdam
Stap 2. Klik op de button 'datalek melden'
Stap 3. Vul het datalekformulier in

7. Bewaartermijnen

Persoonsgegevens mogen niet langer worden bewaard dan dat noodzakelijk is. Persoonsgegevens die zijn verzameld voor het vaccineren of testen van cliënten zijn onderdeel van het medisch dossier van de cliënt. Hiervoor geldt (volgens de Wgbo) een bewaartermijn van 20 jaar. Voor persoonsgegevens die zijn verzameld voor het uitvoeren van een BCO geldt een bewaartermijn van 5 jaar. Dit volgt uit de Wpg.

Testen: Op basis van de Tijdelijke wet coronatoegangsbewijzen (art.2) is bepaald dat positieve testuitslagen maar 1 jaar bewaard worden en negatieve testuitslagen maar 4 weken, gerekend vanaf het moment dat de test is afgenomen. Daarmee wordt voor de bewaartermijnen voor testuitslagen in CoronIT en HPzone dus afgeweken van de wettelijk bepaalde termijn in de Wgbo en in de Selectielijst archiefbescheiden gemeenten en intergemeentelijke organen 2020.

Vaccinatie: Voor de registratie van vaccinatiegegevens blijft de termijn van 20 jaar wel overeind.

Inkomende/uitgaande informatie (zoals e-mail) valt onder een wettelijk bewaartermijn zoals die van de Wgbo en Wpg, dan dient deze informatie in het juiste dossier te worden opgenomen.

8. Privacy beleid GGD

Hieronder staan hyperlinks naar de privacyverklaringen die gelden voor Team Corona:

- GGD: https://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/privacy/
- Testen: https://ggdghor.nl/privacyverklaring-testenopcoronavirus/
- Vaccineren: https://ggdghor.nl/privacyverklaring-vaccinatie_coronavirus/
- BCO: https://ggdghor.nl/wpcontent/uploads/2020/05/Privacy_Verklaring_BCO_April2021_Final.pdf

9. FAQ Privacy & BCO

1. Hoe borg ik de privacy van mijn medewerkers bij een inzageverzoek van het log-overzicht?

In privacywet- en regelgeving wordt een getrapte manier voor het verschaffen van inzage in de loggegevens beschreven. Daarbij wordt in reactie op het inzageverzoek in het log-overzicht allereerst de naam van de verantwoordelijke (bijv. een afdelingshoofd of directeur) getoond. Als de cliënt een vervolgvraag stelt over een specifieke handeling/gebeurtenis uit het log-overzicht, dan kan en moet de zorgorganisatie de belangen van de medewerker die het betreft én de belangen van de cliënt tegen elkaar

CONCEPT

afwegen. Afhankelijk van de omstandigheden en de belangen die spelen, kan ervoor gekozen worden of de naam van de medewerker bekend wordt gemaakt. Deze inschatting wordt per casus gemaakt. Hiermee worden zowel de belangen van de cliënt alsook de belangen van de medewerker in het oog gehouden.

2. Er is behoefte aan een overzicht van alle persoonsgegevens en een korte uitleg met welke reden wij deze als GGD uitvragen en bewaren. Zo kan context geboden worden aan de medewerkers van de coronateams maar kan ook als uitleg gegeven worden aan burgers.
In de privacy verklaringen van de respectievelijke handelingen, Testen, BCO & Vaccineren staat aangegeven waarom wij welke gegevens verzamelen. (https://www.ggd.amsterdam.nl/privacy-ggd-amsterdam/privacyverklaringen-corona-covid-19/ of zie Bijlage 3,4,5)

3. Wat zijn de richtlijnen voor telefonische ID-verificatie bij het inplannen van afspraken en het doorgeven van uitslagen? In principe kan een persoon zich alleen identificeren via DigiD of door live een ID te tonen.
Een zorgaanbieder die via de telefoon of via een elektronisch weg zorg wil verlenen, kan onder voorwaarden zorg verlenen zonder dat de identiteit van de patiënt is vastgesteld met een identiteitsbewijs. Daarvoor gelden twee voorwaarden:

(1) De zorgaanbieder moet de identiteit controleren door naar bepaalde persoon-identificerende gegevens te vragen. Dit betreft:

- geslachtsnaam;
- voornamen;
- geboortedatum;
- postcode van het woonadres;
- huisnummer van het woonadres.

(2) De zorgaanbieder moet bij het verstrekken van persoonsgegevens aan andere zorgaanbieders, indicatieorganen of zorgverzekeraars vermelden dat geen identiteitscontrole heeft plaatsgevonden.

4. Worden e-mails binnen de GGD (naar collega's met een ggd e-mailadres) automatisch veilig verzonden of moet je ook bij collega's op de knop 'veilig verzenden' klikken?
GGD Amsterdam medewerkers (@ggd.amsterdam.nl) kunnen binnen de GGD Amsterdam werkomgeving (GGD@Work) veilig met elkaar mailen, zonder de "veilig verzenden" knop te gebruiken. Alle andere overige e-mailadressen, dus geen @ggd.amsterdam.nl e-mailadressen, of mailen bij de GGD@Work omgeving, dan wel de knop "veilig verzenden" gebruiken.

TIP: Gebruik altijd de 'veilig verzenden' knop, mits een 06-nummer aanwezig is! Is het niet mogelijk om veilig te verzenden overleg dan met je coördinator hoe je dit moet aanpakken.

5. Wat doet de GGD aan het tegengaan van gebruik van werkgerelateerde programma's op privé apparaten? In een thuiswerkhandleiding van de GGD die online te vinden is staat een link hoe je met inlognaam en wachtwoord bij je GGD-mail kunt komen zonder 2-staps verificatie en zonder in Citrix te zijn ingelogd. Aangezien er persoonsgegevens per mail worden verstuurd is het niet wenselijk dat gegevens onverhoopt worden gedownload op privé apparaten.
Vanuit GGD Amsterdam is het technisch nog niet mogelijk om af te dwingen dat er geen bedrijfs- en/of persoonsgegevens lokaal worden opgeslagen op privé devices. Hiervoor dient er binnen Team Corona

CONCEPT

specifieke werkafspraken gemaakt worden, dat er niks lokaal op privé en/of werk devices opgeslagen mag worden.

6. Hoe gaan we om met de vele datalekken die er wekelijks geconstateerd worden? Dit is een flinke administratieve rompslomp. Bijvoorbeeld datalekken die bij ons terecht komen via landelijk en wij niet direct kunnen melden, maar via de servicedesk moeten melden bij GGD GHOR in de hoop dat er iets mee gedaan wordt.

De beste manier om administratieve rompslomp te voorkomen is toezien op zorgvuldig handelen en daarmee ervoor te zorgen dat er geen datalekken worden veroorzaakt. Verder zijn we wettelijk verplicht een datalekregister bij te houden. Dus toch via TOPdesk blijven melden.

7. Hoe lang blijven index dossiers bij ons in HPZone bewaard ?

De GGD bewaart de persoonsgegevens die verwerkt worden in kader van het bron- en contactonderzoek zolang noodzakelijk is voor een effectieve uitvoering, maar ten hoogste vijf jaar, zoals voorgeschreven in artikel 29 van de Wet Publieke Gezondheid. Na deze periode worden jouw gegevens verwijderd of geanonimiseerd (onherkenbaar gemaakt). We bewaren je persoonsgegevens niet langer dan nodig, of dan aangegeven in de wet. Behalve als wij daar jouw toestemming voor hebben.

8. Stellen wij in alle gevallen, dus ook bij 'kleine' datalekken' de index op de hoogte? Of maken we hierin een afweging per case?

Een eventuele melding aan betrokkenen moet onverwijld plaatsvinden. Inbreuken zonder een hoog risico voor de persoonlijke levenssfeer van de betrokken natuurlijke personen hoeven niet aan betrokkenen te worden gemeld. Met andere woorden, we maken hierin een afweging per case. Voor meer informatie, zie werkinstructie Datalek melden.

Vragen

Vragen over deze werkinstructie kunnen worden gesteld aan 5.1,2,e@ggd.amsterdam.com

10. Bijlagen

a. Modelbrief ontvangstbevestiging verzoek

CONCEPT