Datum: 05-2024
Revisie: 05-2025

Intern privacybeleid
Voor de verwerking van persoonsgegevens

Inhoudsopgave

1 Introductie ... 3

1.1 Contactgegevens ... 3

2 Privacybeleid ... 4

2.1 Verwerkingsregister ... 4

3 Type persoonsgegevens en doeleinden ... 5

3.1 Cliënten ... 5

Veilig Incident Melden (VIM) ... 6

Toezicht en handhaving ... 6

3.2 Medewerkers ... 6

4 Informatieplicht ... 7

5 Rechten van betrokkenen ... 8

6 Derde partijen ... 8

7 Beveiliging ... 9

8 Datalekken ... 10

9 Bewaartermijnen ... 11

9.1 Cliënt/cliëntgegevens ... 11

9.2 Gegevens medewerkers ... 11

9.3 Overige persoonsgegevens ... 11

10 Doorgifte buiten EER ... 12

Bijlage I Privacyverklaring cliënten ... 14

Bijlage II Privacyverklaring medewerkers en sollicitanten ... 14

Bijlage III Protocol en stappenplan bij datalekken ... 13

Bijlage IV Standaardbrief incidenten ... 18

1 Introductie

Dit is het privacybeleid (hierna: het “Privacybeleid”) van G’woon Samen (hierna: de “Organisatie”). Dit Privacybeleid ziet zowel op het verzamelen en verwerken van persoonsgegevens die in verband met de hulp- en zorgverlening aan cliënten worden verwerkt, als op gegevens van medewerkers die binnen de Organisatie worden gebruikt. Het Privacybeleid beschrijft op welke wijze de Organisatie met deze gegevens omgaat en welke protocollen en processen zij binnen de Organisatie heeft geïmplementeerd om ervoor te zorgen dat de veiligheid van de gegevens gewaarborgd is en dat aan de vereisten van de Algemene verordening gegevensbescherming (“AVG”) wordt voldaan.

In dit Privacybeleid komen de volgende onderwerpen aan bod.

- Verwerkingsregister
- Type persoonsgegevens en doelen
- Informatieplicht
- Rechten van betrokkenen
- Derde partijen
- Beveiliging
- Datalekken
- Bewaartermijnen
- Doorgifte van persoonsgegevens

De protocollen en overige documenten waarnaar in dit Privacybeleid wordt verwezen, zijn als bijlage aan het Privacybeleid gehecht.

Om ervoor te zorgen dat dit Privacybeleid blijft aansluiten bij de verwerking van persoonsgegevens binnen de Organisatie, zal het Privacybeleid elk jaar worden geëvalueerd. Aan de hand van die evaluatie zal, indien vereist, het Privacybeleid en de hieraan gehechte protocollen en documenten worden aangepast. Indien op een moment voor de evaluatie duidelijk wordt dat het Privacybeleid aanpassing behoefd, zal de Organisatie de vereiste aanpassingen op dat moment al doorvoeren.

Als Organisatie zijn wij verantwoordelijk voor de verwerking van uw persoonsgegevens. Indien u na het doornemen van ons Privacybeleid, of in algemenere zin, vragen heeft hierover of contact met ons wenst op te nemen kan dit via onderstaande contactgegevens.

1.1 Contactgegevens

G’woon Samen
Kanaalweg- Oost 36
7691 CE Bergentheim
info@gwoonsamen.nl

2 Privacybeleid

G'woon Samen hecht veel waarde aan de bescherming van uw persoonsgegevens. In dit Privacybeleid willen we heldere en transparante informatie geven over hoe wij omgaan met persoonsgegevens.

Persoonsgegevens
alle informatie die direct of indirect tot een persoon te herleiden is. Gegevens die feitelijke informatie geven over een persoon zijn bijvoorbeeld iemands naam, geboortedatum of geslacht. Echter, denk ook aan: mailadres, telefoonnummer, huisadres, werkgever, opleidingen of medische dossiers.

2.1 Verwerkingsregister

De Organisatie houdt een verwerkingsregister bij. Dit register bevat onder meer een beschrijving van de (categorieën) persoonsgegevens die binnen de organisatie worden verwerkt, de doelen waarvoor ze worden verwerkt, de derden aan wie de gegevens worden verstrekt, de bewaartermijn van de gegevens en de technische en organisatorische maatregelen die zijn genomen om de gegevens te beschermen.

In het verwerkingsregister dient voor elke verwerking opgenomen te worden welke persoonsgegevens worden verzameld en voor welk doel ze worden gebruikt. Voorbeelden van gegevensverwerkingen zijn:

- het registreren van persoonsgegevens om een nieuwe cliënt in te schrijven;
- het vastleggen en bijhouden van persoonsgegevens van een cliënt in het kader van de begeleiding van de cliënt;
- het gebruiken van persoonsgegevens ten behoeve van facturatie;
- het verstrekken van (medische) gegevens aan een derde, bijvoorbeeld ten behoeve van een doorverwijzing; of
- het vastleggen van persoonsgegevens voor het aanleggen en bijhouden van een dossier.

Binnen de Organisatie heeft het directie en management en medewerker financiële bedrijfsvoering toegang tot het register. Zij kunnen het register raadplegen en daar wijzigingen in aanbrengen.

Het register wordt door de Organisatie continue en actief bijgehouden. Wijzigingen in de verwerking van persoonsgegevens worden direct in het register doorgevoerd. Tijdens de jaarlijkse evaluatie zal ook worden beoordeeld of het register nog altijd accuraat is of dat aanpassingen in het register vereist zijn.

3 Cameratoezicht

Op de locatie in Bergentheim, Kanaalweg Oost 36 7691CE, Bergentheim is er sprake van cameratoezicht. Er zijn buitenshuis 4 camera's rondom de locatie. De camerabeelden worden maximaal 24 uur bewaard en dan worden ze automatisch verwijderd. De beelden dienen uitsluitend voor eigen gebruik. Dat wil zeggen dat de beelden niet met derden gedeeld zullen worden. Jongeren die komen wonen in Bergentheim wordt bij aanmelding verteld dat deze camera's er hangen.

Bij de locatie in Balkbrug, Den Huizen 3 7707 PL Balkbrug, is er sprake van camera toezicht. Er zijn buitenshuis 3 camera's rondom de locatie. De camerabeelden worden maximaal 24 uur bewaard en worden daarna automatisch verwijderd. Beelden zijn uitsluitend voor eigen gebruik en worden dus

niet met derden gedeeld. Kindern en voogden worden bij aanmelding hiervan op de hoogte gebracht.

Bij locatie Dina's Fellows hangen diverse camera's zowel in als rondom het pand om toezicht te houden op eigendommen van de winkel The Fellowship of Acoustics (TFOA) waar Dina's Fellows ruimte huurt om dagbestedingsactiviteiten te kunnen uitvoeren. Onze cliënten worden bij aanmelding bij de dagbesteding geattendeerd op deze camera's. De camerabeelden worden 2 weken bewaard en daarna automatisch verwijderd. Tevens hangt er ook bij de ingang van het pand een bord waarop men wordt geattendeerd op het aanwezig zijn van camera's in en rondom het pand.

4 Type persoonsgegevens en doeleinden

Binnen de Organisatie worden persoonsgegevens van twee hoofdcategorieën personen verwerkt: i) de cliënten; en ii) de medewerkers.

3.1 Cliënten

Cliënten kunnen zorg aanvragen door telefonisch contact op te nemen of het online inschrijfformulier in via de aanvragen via de mail. Hierbij wordt de cliënt verzocht gegevens te verstrekken die vereist zijn voor inschrijving: soort zorg, naam en telefoonnummer. Vervolgens wordt door de zorg coördinator beoordeeld of er een intake wordt ingepland of dat er wordt doorverwezen naar andere zorgverleners. Indien van toepassing wordt er telefonisch contact met de cliënt opgenomen voor het maken van een intake afspraak.

De intake afspraak/ het toelatingsgesprek omvat een korte kennismaking door de zorg coördinator of een hulpverlener aan de hand van een vragenlijst.

Na de intake wordt er samen met de cliënt een ondersteuningsplan opgesteld en worden afspraken ingepland voor de begeleiding.

Indien de cliënt afkomstig is van een andere Organisatie, kunnen persoonsgegevens van die andere Organisatie worden verkregen. De cliënt dient deze gegevens zelf op te vragen of toestemming te geven dat deze verstrekt mogen worden.

Alle gegevens die de Organisatie verkrijgt in het kader van het inschrijven van een cliënt, worden opgeslagen in een electronisch cliëntendossier (MEXTRA)

Naast de gegevens vereist voor inschrijving bij de Organisatie, verwerkt de Organisatie gegevens die verband houden met de (evaluatie van) begeleiding van de cliënt. Het gaat daarbij onder meer om afspraken, gegevens omtrent de uitgevoerde begeleiding en verwijzingen naar andere zorgverleners. Al deze gegevens worden in het dossier opgeslagen.

Verder worden gegevens gebruikt om de factuur op te stellen. De factuur is voorzien van een factuurnummer, evt gemeentecode, periode, evt referentienummer, de naam van de cliënt, geboortedatum, BSN es, start- en einddatum van de declaratie, de betreffende wet, productcode en uitleg hiervan en ten slotte het bedrag.

Alle gegevens die over de cliënt worden verzameld, worden gebruikt met als doel de hulp- en zorgverlening voor de cliënt.

Bij intercollegiale toetsing binnen een Organisatie of instelling kunnen gegevens worden gebruikt en verstrekt. De cliënt wordt daar van tevoren van op de hoogte gebracht.

Veilig Incident Melden (VIM)

Binnen de Organisatie is het management degene die zorgdraagt voor de procedure om incidenten te melden, zich inzet voor een cultuur binnen de Organisatie dat incidenten worden gemeld en die ervoor zorgt dat meldingen worden geanalyseerd.

Meldingen van incidenten kunnen digitaal worden gedaan in het ECD. De melding bevat zowel persoonsgegevens van de betreffende medewerker van de Organisatie als de cliënt in kwestie.

Het management analyseert de melding en behandelt deze vertrouwelijk. Indien nodig vraagt zij nadere informatie aan de melder. Van het incident wordt aantekening gemaakt in het cliëntendossier van de cliënt, waarin wordt vermeld: de aard en toedracht van het incident; het tijdstip waarop het incident heeft plaatsgevonden; en de namen van de bij het incident betrokken zorgverleners.

De Organisatie zorgt dat meldingen vertrouwelijk worden behandeld en dat de meldingen zo worden bewaard dat deze niet toegankelijk zijn voor anderen.

Toezicht en handhaving

Op grond van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) maakt de Organisatie bij de Inspectie voor de Gezondheidszorg (IGZ) melding van eventuele calamiteiten die bij de zorgverlening hebben plaatsgevonden. Ook meldt de Organisatie het bij de IGZ als er geweld bij de zorgverlening heeft plaatsgevonden of als de arbeidsrelatie met een individuele zorgverlener is beëindigd vanwege ernstige functioneringsproblemen.

Op grond van de wet komt aan de IGZ een aantal bevoegdheden toe bij het houden van toezicht op specifieke volksgezondheidswetten. Bij onderzoek dat specifiek is gericht op individuele casuïstiek, heeft de IGZ recht op inzage in medische dossiers voor zover deze inzage nodig is voor de uitvoering van haar taken. De Organisatie is dan gehouden om de IGZ inzage te verlenen.

De Nederlandse Zorgautoriteit (NZa) is onder meer belast met markttoezicht, marktontwikkelingen, tarief- en prestatieregulering en met toezicht op de uitvoering van de Zorgverzekeringswet en de Wet langdurige zorg (Wlz). In dat kader kan de Organisatie in sommige gevallen verplicht zijn om op verzoek bepaalde gegevens aan de NZa te verstrekken. Het kan hier gaan om identificerende gegevens die de Organisatie eigenaren betreffen, om andere identificerende persoonsgegevens en om medische persoonsgegevens van cliënten.

3.2 Medewerkers

In het kader van de uitvoering van de arbeidsovereenkomst, verwerkt de Organisatie ook persoonsgegevens van haar medewerkers. De arbeidsovereenkomst en daarmee samenhangende gegevens worden opgeslagen in het personeelsdossier. Deze gegevens worden in eerste instantie gebruikt voor het vaststellen en uitbetalen van het salaris van de medewerkers.

In het personeelsdossier kunnen ook gegevens omtrent eventuele klachten, waarschuwingen, beoordelingen en verzuimfrequentie worden opgeslagen.

De toegang tot de personeelsdossiers is beveiligd. Binnen de Organisatie heeft enkel de directie toegang tot het personeelsdossier.

De Organisatie is wettelijk gehouden bepaalde persoonsgegevens van medewerkers aan derde partijen te verstrekken. Deze verstrekking aan derde partijen heeft de volgende doeleinden:

- Bij indiensttreding wordt aan de collectieve zorgverzekeraars en andere collectieve verzekeraars de datum van indiensttreding, NAW-gegevens en het BSN van medewerkers doorgegeven.
- Ziek- en herstelmeldingen worden doorgegeven aan de Arbodienst.
- Bij uitdiensttreding vanwege ziekte en bij zwangerschapsverlof worden gegevens van medewerkers aan het UWV doorgegeven in verband met het verkrijgen van een vangnetuitkering, waaronder salaris, pensioenpremie, prepensioen, hiaatverzekering, de NAW-gegevens en het BSN.
- Aan pensioenfondsen en andere daaraan gelieerde instellingen en organisaties worden eveneens gegevens verstrekt.

Gegevens omtrent het functioneren van medewerkers worden ook verwerkt in het kader van individuele kwaliteitsverbetering. De verzamelde gegevens worden dan gebruikt voor het coachen en trainen van medewerkers met het doel hen beter te laten functioneren.

Gegevens omtrent het functioneren van medewerkers kunnen ook gebruikt worden voor de beoordeling van de medewerker, bijvoorbeeld in het kader van functioneringsgesprekken. De gegevens die de Organisatie verzamelt om medewerkers te beoordelen, kunnen door de medewerkers worden ingezien waarbij de medewerker kans krijgt om hierop te reageren. De verslaglegging van functioneringsgesprekken dient als uitgangspunt bij een volgend gesprek en wordt benut als managementinformatie.

Tot slot kan het zo zijn dat, in het kader van het verbeteren van de bedrijfsprocessen, binnen de Organisatie, persoonsgegevens van medewerkers worden verwerkt.

Deze categorieën van persoonsgegevens, van zowel de cliënten als de medewerkers, staan samen met de overige categorieën vermeld in het verwerkingsregister.

4 Informatieplicht

De Organisatie stelt de cliënten bij inschrijving op de hoogte van de persoonsgegevens die zij over de cliënt verzamelt en voor welke doeleinden deze persoonsgegevens vervolgens worden gebruikt. Bij de inschrijving via de website wordt tijdens het proces van inschrijving door middel van een hyperlink verwezen naar de privacyverklaring. De privacyverklaring voor cliënten is als Bijlage I aan dit Privacybeleid gehecht en wordt altijd in ook in papierversie verstrekt aan zowel clienten als medewerkers wanneer zij starten met werken bij ons.

Bij indiensttreding wordt aan de medewerkers kenbaar gemaakt voor welke doeleinden hun persoonsgegevens worden verwerkt en wat er van hun in het kader van privacy mag worden verwacht. De privacyverklaring voor medewerkers en sollicitanten is als Bijlage II aan dit Privacybeleid gehecht.

In het kader van art. 7.448 van de WGBO dient de client zo goed mogelijk op de hoogte te worden gebracht betreffende zijn/haar zorgplan en doelen. De cliënt wordt in het nieuwe relatiemodel gezien als gesprekspartner van de hulpverlener. Dit betekent dat de informatieplicht van de hulpverlener wordt aangevuld met de verplichting om tijdig en doorlopend te overleggen met de cliënt over het voorgenomen onderzoek en de voorgestelde behandeling en over de ontwikkelingen omtrent het onderzoek, de behandeling en de gezondheidstoestand van de cliënt. Daarbij komt dat de hulpverlener de cliënt op duidelijke wijze moet informeren op een wijze die past bij zijn bevattingsvermogen.

5 Rechten van betrokkenen

Alle verzoeken, op welke wijze ook binnengekomen (telefonisch, per e-mail, per brief), van een cliënt of medewerker waarin rechten ten aanzien van persoonsgegevens worden ingeroepen, worden verzonden aan de directie via info@gwoonsamen.nl. Verzoeken en alle overige afhandeling worden opgeslagen op de Microsoft server (Rechten van betrokkenen).

Na ontvangst van een verzoek zal de Organisatie eerst de identiteit van de verzoeker verifiëren. De Organisatie kan de verzoeker vragen een kopie van een identiteitsbewijs mee te zenden. De Organisatie zal daarbij aan de verzoeker aangegeven dat het BSN niet mag worden verstrekt en dus van de kopie van het identiteitsbewijs verwijderd moet worden.

Indien de identiteit van de betrokkene is vastgesteld, zal de Organisatie de verzoeker laten weten dat er binnen twee weken op het verzoek zal worden gereageerd. Indien het verzoek complex is, kan deze termijn met maximaal twee maanden worden verlengd. Indien dit het geval is, zal de Organisatie dit binnen de initiële maand aan de verzoeker laten weten.

De directie zal vervolgens vaststellen welk recht precies wordt ingeroepen en verzamelt de in dat kader vereiste informatie. Op basis van deze informatie wordt een verslag opgesteld. Op basis van dit verslag wordt besloten of, en zo ja, op welke wijze aan het verzoek van de verzoeker kan worden voldaan.

Voor de communicatie richting de verzoeker en het treffen van maatregelen naar aanleiding van een verzoek zullen in beginsel geen kosten in rekening worden gebracht bij de verzoeker. Slechts in bepaalde gevallen zal de Organisatie kosten in rekening brengen (een redelijke vergoeding in het licht van de administratieve kosten). Bijvoorbeeld wanneer verzoeker meerdere inzageverzoeken of herhaaldelijk ongegronde verzoeken indient. De Organisatie mag in uitzonderingsgevallen ook weigeren om gevolg te geven aan het verzoek.

Indien gevolg wordt gegeven aan het verzoek van een verzoeker, dienen in bepaalde gevallen ook derde partijen op de hoogte te worden gesteld. Het verslag dient daarom ook de derde partijen te beschrijven die betrokken zijn bij het honoreren van een verzoek van de verzoeker. Dergelijke kennisgevingen laat de Organisatie achterwege als dit onmogelijk blijkt of onevenredig veel inspanning vergt.

De Organisatie heeft zodanige technische en organisatorische maatregelen genomen dat aan verzoeken van verzoekers kan worden voldaan. Zo kan de Organisatie een verzoeker inzage verlenen in de gegevens die over hem/haar worden verzameld, kunnen gegevens worden verwijderd of verbeterd, kan de verwerking van gegevens tijdelijk worden gestaakt, kunnen deze gegevens makkelijk overgezet worden naar een nieuwe aanbieder en wordt er bij de intrekking van toestemming zorg voor gedragen dat de gegevens vanaf dat moment niet weer voor dat doel worden gebruikt.

6 Derde partijen

De Organisatie maakt voor het verwerken van persoonsgegevens gebruik van derde partijen. Het gaat daarbij onder meer om partijen die louter ten behoeve van de Organisatie gegevens verwerken (hierna: “Verwerkers”).

Verwerker
een partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Deze partij bepaalt dus **niet** voor welk doel gegevens worden verzameld en gebruikt. Voorbeelden zijn de partijen die het salarisadministratiesysteem en het cliëntsysteem aanbieden.

Verwerkingsverantwoordelijke
degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dat is dus de partij die bepaalt wat er met de gegevens gebeurt. De Organisatie is als verwerkingsverantwoordelijke aan te merken.

Met deze Verwerkers wordt een verwerkersovereenkomst afgesloten waarin onder meer de mate van beveiliging van de persoonsgegevens die de Verwerker voor de Organisatie verwerkt wordt beschreven. Ook bevatten de verwerkersovereenkomst bepalingen omtrent het uitvoeren van een audit bij de Verwerker en de procedure die moet worden gevolgd als van een incident omtrent persoonsgegevens sprake is.

In de Organisatie wordt van de volgende Verwerkers gebruikgemaakt:

- Mextra
- Carres (s Heerenloo)
- Countus
- Exite ICT

Persoonsgegevens van cliënten of medewerkers worden aan andere verwerkingsverantwoordelijken doorgegeven wanneer dat wettelijke vereist is, noodzakelijk is in het kader van hulp- en zorgverlening van de cliënt (verwijzingen) en voor intercollegiaal overleg. Buiten deze situatie worden persoonsgegevens niet aan andere verwerkingsverantwoordelijken verstrekt zonder voorafgaande uitdrukkelijke toestemming van de cliënt of medewerker. Dat is alleen anders indien er een wettelijke verplichting tot verstrekking bestaat of indien de gegevens in het verlengde van de zorg- en hulpverlening gedeeld moeten worden, bijvoorbeeld in het kader van intercollegiaal overleg. Daarbij geldt dat alleen de strikt noodzakelijk geachte gegevens worden verstrekt.

7 Beveiliging

De Organisatie hecht veel waarde aan de beveiliging van zowel de cliëntgegevens als de gegevens van haar medewerkers. De Organisatie heeft daarom passende technische en organisatorische maatregelen genomen om deze persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Voor zover de Organisatie gebruik maakt van Verwerkers zijn met deze Verwerkers afspraken gemaakt over de te nemen technische en organisatorische maatregelen.

De Organisatie heeft op grond van de verwerkersovereenkomst het recht de door de Verwerker getroffen maatregelen periodiek te auditen, testen, beoordelen en evalueren om zo te bepalen of de overeengekomen maatregelen worden nageleefd en of deze nog doeltreffend zijn en om deze zo nodig aan te laten passen.

De Organisatie hanteert in aanvulling op het bovenstaande ook interne beveiligingsmaatregelen. Het gaat daarbij onder meer om de volgende maatregelen:

- Persoonsgegevens worden op een beveiligde wijze uitgewisseld [en niet via WhatsApp, Dropbox of Gmail];
- De website (webadres) is beveiligd met een TLS 1.2 certificaat;
- Persoonsgegevens worden niet op USB sticks of andere mobiele dragers gekopieerd tenzij de persoonsgegevens worden versleuteld;
- Er is een wachtwoordbeleid. Wachtwoorden zijn voldoende sterk en worden periodiek vervangen;
- Binnen de Organisatie zijn processen ingericht die aangeven wat er moet gebeuren indien een incident inzake persoonsgegevens zich voordoet of indien cliënten of medewerkers een beroep op hun rechten doen;
- Binnen de Organisatie zijn medewerkers geïnformeerd over het belang van de bescherming van persoonsgegevens;
- Binnen de Organisatie is een clean desk policy geïmplementeerd om de kans op fraude en datalekken te verminderen. Documenten met persoonsgegevens worden niet onbeheerd achter gelaten op een bureau of bij de printer;
- Binnen de Organisatie is het niet toegestaan, zonder toestemming van de Organisatie, software te downloaden en/of om firewalls of virusscanner aan te passen of te verwijderen;
- Alle personen die namens de Organisatie van gegevens kennis kunnen nemen, zijn gehouden aan geheimhouding daarvan en hebben hiervoor getekend in hun arbeidsovereenkomst;
- Apparaten als laptops en mobiele telefoons worden niet onbeheerd achtergelaten, worden versleuteld opgeslagen en verlies/diefstal dient direct te worden gemeld bij de Organisatie;
- Alleen directie heeft toegang tot personeelsdossiers;
- Toegang tot het pand is alleen mogelijk met aan medewerkers verstrekte sleutels.

Binnen de Organisatie worden dagelijks meerdere back-ups gemaakt van de Microsoft server. De back-up wordt buiten de organisatie bewaard op een harde schijf. Hiermee realiseert de Organisatie dat in het geval van een incident met persoonsgegevens (bijvoorbeeld in het geval van ransomware) een recente back-up teruggezet kan worden zodat persoonsgegevens niet blijvend verloren gaan.

Uitgangspunt binnen de Organisatie is dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld. Zo vraagt de Organisatie niet meer informatie uit bij de cliënt dan noodzakelijk is voor zorg- en hulpverlening. Ook bij het inschakelen van derde partijen, beoordeelt de Organisatie of de door die derde partij aangeboden dienst aansluit bij het doel dat de Organisatie voor ogen heeft en er niet meer persoonsgegevens worden verzameld dan daarvoor nodig is (*privacy by design en privacy by default*).

8 Datalekken

De Organisatie heeft passende technische en organisatorische maatregelen genomen die tot doel hebben de kans op verlies of onrechtmatige verwerking van persoonsgegevens zo veel mogelijk te beperken. Ondanks deze maatregelen bestaat de kans dat zich toch een incident met betrekking tot persoonsgegevens voordoet. Om ervoor te zorgen dat er zo snel mogelijk opgetreden kan worden om het incident te beëindigen en de schade zo veel mogelijk te beperken, maakt de Organisatie gebruik van een protocol en stappenplan datalek melden, welke als Bijlage III bij dit Privacybeleid is gevoegd.

Elk incident met betrekking tot persoonsgegevens moet worden gemeld aan de directie via info@gwoonsamen.nl. De directie zal vervolgens bepalen of:

- er inderdaad sprake is van een incident dat betrekking heeft op persoonsgegevens

- welke maatregelen genomen moeten worden om het incident te stoppen en de gevolgen te beperken
- er een externe partij moet worden ingeschakeld om bij de oplossing van het incident te assisteren
- het incident aan de Autoriteit Persoonsgegevens moet worden gemeld. De melding aan de Autoriteit Persoonsgegevens zal vervolgens binnen 72 uur nadat de Organisatie op de hoogte is geraakt van het incident plaatsvinden
- degenen op wie de persoonsgegevens betrekking hebben, moeten (mogelijk) worden geïnformeerd over het incident
- welke maatregelen er genomen moeten worden om herhaling van het incident te voorkomen

Voor het geval ook betrokkenen geïnformeerd moeten worden over een incident, hanteert de Organisatie een standaardbrief welke als Bijlage IV bij dit Privacybeleid is gevoegd.

Aangezien de kans bestaat dat een Verwerker als eerste op de hoogte raakt van een (potentieel) incident, is in de Verwerkersovereenkomst afgesproken dat de Verwerker de Organisatie zo snel mogelijk op de hoogte stelt van een incident. Ook zijn er afspraken gemaakt over het oplossen van het incident en het verstrekken van nadere gegevens.

De Organisatie documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Hiervoor kan gebruik worden gemaakt van het datalekkenregister. Dit register wordt opgeslagen op de Microsoft server (Datalekken).

9 Bewaartermijnen

De Organisatie hanteert een beleid voor het bewaren van persoonsgegevens. Persoonsgegevens die niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld en tevens niet op grond van andere wetgeving bewaard moeten worden, worden door de Organisatie verwijderd. De persoonsgegevens dienen in dat geval ook uit eventuele back-ups, archieven en andere systemen te worden verwijderd.

9.1 Cliënt/cliëntgegevens

Cliëntgegevens worden 1 jaar bewaard vanaf de laatste wijziging in het document en client uit organisatie stapt.

9.2 Gegevens medewerkers

De Organisatie bewaart gegevens van medewerkers voor zover vereist op basis van fiscale boekhoud- en administratieplicht gedurende een periode van zeven (7) jaar.

Voor zover de betreffende gegevens niet vallen onder de fiscale boekhoud- en administratieplicht, hanteert de Organisatie de volgende bewaartermijnen:

- Loonadministratie (gedurende 1 jaar na uitdiensttreding)
- Loonbelastingverklaring (gedurende 1 jaar na uitdiensttreding)
- Kopie identiteitsbewijs werknemer (gedurende 1 jaar na uitdiensttreding)
- Personeelsdossier (gedurende 1 jaar naar uitdiensttreding)

9.3 Overige persoonsgegevens

Gegevens die met behulp van camerabeelden worden verzameld, worden gedurende 24 uur bewaard tenzij langer bewaren noodzakelijk is in verband met geconstateerde strafbare feiten.

Ten aanzien van facturen die niet als medische behandelgegevens kwalificeren, bijvoorbeeld facturen aan/van derde partijen, bewaart de Organisatie deze in verband met de omzetbelasting gedurende een periode van zeven (7) jaar.

Gegevens die worden verzameld in het kader van sollicitaties worden uiterlijk vier (4) weken na het einde van de sollicitatieprocedure verwijderd. Sollicitanten kunnen toestemming geven om gegevens langer te bewaren. Bijvoorbeeld omdat er mogelijk op een later tijdstip een passende functie voor hem of haar vrijkomt. Hiervoor wordt een termijn van maximaal 1 jaar na beëindiging van de sollicitatieprocedure gehanteerd.

10 Doorgifte buiten EER

De Organisatie slaat gegevens van cliënten en medewerkers in beginsel niet op buiten de Europese Economische Ruimte (EER).

Indien de Organisatie persoonsgegevens toch buiten de EER opslaat, bijvoorbeeld omdat een Verwerker van de Organisatie daar gevestigd is, zorgt de Organisatie er voor dat de doorgifte alleen plaatsvindt als:

- de Europese Commissie heeft aangegeven dat het betreffende land een passend beschermingsniveau biedt;
- de EU standard contractual clauses zijn overeengekomen;
- het privacy shield van toepassing is; of
- een andere vrijstelling van toepassing is.

Bijlage I Protocol en stappenplan bij datalekken

Protocol

Dit protocol beschrijft de stappen met daarin te nemen maatregelen die binnen G'woon Samen moeten worden gezet bij een datalek volgens de meldplicht datalekken van de Algemene Verordening Gegevensbescherming (AVG).

Reikwijdte van de meldplicht datalekken

Indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens als bedoeld in artikel 33 en 34 van de AVG, die leidt tot een (aanzienlijke kans op) ernstige nadelige gevolgen voor de rechten en vrijheden van betrokkene(n)[1] dan moet dit worden doorgegeven aan de Autoriteit Persoonsgegevens (AP).

Datalekken kunnen ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden; verstrekken van username/wachtwoord aan collega's en/of externe partijen);
- calamiteit (brand, wateroverlast);
- verloren USB-stick of laptop;
- verzenden van e-mail met e-mailadressen van alle geadresseerden.

Meldingen

Een datalek kan door een medewerker of een verwerker van G'woon Samen worden ontdekt. Deze ontdekking moet **direct** worden doorgegeven aan de directie via info@gwoonsamen.nl. Zij zullen vervolgens over gaan tot de beoordeling of sprake is van een datalek aan de hand van het stappenplan datalekken.

Hierbij is aandacht voor de volgende aspecten:

1. zijn er persoonsgegevens (van natuurlijke personen) gelekt en zo ja, hoeveel personen betreft het?
2. zijn er bijzondere (zoals medische of financiële gegevens of BSN/kopie legitimatiebewijs) gelekt?
3. kan dit datalek ernstige gevolgen hebben voor de rechten en vrijheden van de betrokkene(n)?
4. wat is de oorzaak dat dit incident heeft plaatsgevonden?
5. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures?
6. is de organisatie verwijtbaar?

Indien sprake is van een ernstig datalek, welke leidt tot ernstige nadelige gevolgen voor de bescherming van persoons- gegevens of als een aanzienlijke kans bestaat dat dit gebeurt, dan zal de directie binnen 2 dagen maar niet later dan 72 uur na ontdekking zorg dragen voor een melding bij de AP.

[1] Een enkele tekortkoming of kwetsbaarheid in de beveiliging is geen datalek. Dit is wel het geval wanneer redelijkerwijs niet kan worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid.

Let op: een datalek moet binnen 72 uren worden gemeld aan de AP (avonden en weekenden meegeteld!). De 72 uren gaan in op het moment van het detecteren van het datalek.

De AP zal contact met G'woon Samen opnemen mocht na een melding aanleiding zijn om nadere stappen te ondernemen. Hierbij zal met name de herkomst van de melding worden geverifieerd en kan G'woon Samen aanwijzingen van de AP krijgen.

Wanneer vaststaat dat een datalek bij de AP moet worden gemeld dan dient hierna te worden beoordeeld of een datalek ook aan betrokkene(n) moet worden gemeld. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. In het geval van G'woon Samen kunnen de betrokkenen de persoonsgegevens van klanten en medewerkers zijn. Medewerkers van G'woon Samen worden als betrokkenen aangemerkt indien een datalek hun persoonsgegevens betreft. Een betrokkene moet ook onverwijld in kennis worden gesteld van de inbreuk (middels de standaardbrief incidenten). Indien de inbreuk waarschijnlijk geen ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene(n) of wanneer genomen technische beschermingsmaatregelen (bijvoorbeeld encryptie) voldoende bescherming bieden, kan melding van de datalek aan de betrokkene(n) achterwege blijven.

Verder zal de directie een overzicht bijhouden van alle datalekken binnen G'woon Samen. Per datalek wordt in het overzicht aangegeven wat de feiten en gegevens zijn van de aard van de inbreuk. Een datalek wordt voor minimaal 1 jaar in het overzicht bewaard.

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker of verwerker van G'woon Samen, die direct of indirect kennis draagt of krijgt van een datalek, is verplicht dit direct te melden;
2. De directie is verantwoordelijk voor het onderzoeken van het incident;
3. De directie is verantwoordelijk voor de beoordeling of een datalek aan de AP gemeld moet worden respectievelijk of een datalek aan de betrokkene moet worden gemeld;
4. De directie is verantwoordelijk voor de melding van datalekken bij de AP;
5. De directie is verantwoordelijk voor het bijhouden van een overzicht van alle datalekken die onder de meldplicht vallen voor minimaal 1 jaar;
6. De directie is verantwoordelijk voor het ondernemen van preventieve en repressieve maatregelen om datalekken te voorkomen.

Stappenplan

1 Heeft G'woon Samen een datalek gehad?

1.1 Wat zijn persoonsgegevens?

Persoonsgegevens zijn alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon (dus geen vereniging of bedrijf) in de zin van de wet. Gegevens die feitelijke informatie geven over een persoon zijn bijvoorbeeld iemands naam, geboortedatum of geslacht.

1.2 Wat is een datalek?

Een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan. Ook is sprake van een datalek als niet redelijkerwijs kan worden uitgesloten dat deze gegevens onrechtmatig kunnen/zullen worden verwerkt. Bij een datalek zijn persoonsgegevens van uw organisatie verloren gegaan of in verkeerde handen terechtgekomen.

1.3 Wat is er gebeurd?

De meest voorkomende situaties bij datalekken staan hieronder, met hoofdoorzaken (linkerkant) en onderliggende oorzaken (rechterkant). Geef met vinkjes aan wat er is gebeurd.

Apparaat gestolen of verloren met daarop persoonsgegevens:

- Laptop
- Telefoon
- USB
- Papier
- Anders: _____

Inbraak in een gebouw of computer waar persoonsgegevens van uw organisatie opgeslagen zijn:

- Gegevens zijn meegenomen
- Gegevens zijn mogelijk bekeken
- Anders: _____

Persoonsgegevens van uw organisatie zijn zichtbaar geworden voor niet-geautoriseerde personen:

- Verkeerd e-mailadres gebruikt
- BCC en/of CC fout
- Post aan verkeerde personen gestuurd
- Anders: _____

Er zijn persoonsgegevens van uw organisatie verloren gegaan door:

- Crash van een PC
- Brand in een datacentrum
- Anders: _____

Datalek bij verwerker:

- Anders: _____

Ander datalek:

_____
_____

2 Uw organisatie heeft inderdaad een datalek gehad!

2.1 Beschrijf de gebeurtenis.

Wat is er gebeurd? Beschrijf de gebeurtenis zoals hieronder is aangegeven. Maak gebruik van het ingevulde oorzakenformulier (1.3) en houd die volgorde aan.

TIP: Informeer bij een datalek altijd de directie. Zij zijn n.a. verantwoordelijk en aansprakelijk.

2.2 Over hoeveel personen gaat het?

Over hoeveel verschillende personen is informatie via het datalek mogelijk in verkeerde handen gekomen? Geef het aantal hieronder aan.

2.3 Is er bewijsmateriaal veiliggesteld?

Heeft u bewijsmateriaal beschreven, bewaard of op andere manier veiliggesteld waarmee u meer kunt aantonen over het datalek? Bewaar dit goed, want er kan naar gevraagd worden.

2.4 Is de politie geïnformeerd?

Als u ‘gehackt’ bent of er is fysiek ingebroken, dan is er sprake van een strafbaar feit. Informeer in zo'n geval altijd en direct de politie.

2.5 Samenvatting.

Uw organisatie heeft inderdaad een datalek gehad.

Wat is er gebeurd? Geef een uitgebreide beschrijving.

_____
_____
_____
_____

Van .. personen zijn de persoonsgegevens betrokken bij dit datalek.

☐ Er is bewijsmateriaal en dit is veiliggesteld.

☐ Er is contact opgenomen met de politie.

3 Beoordeling van het datalek

3.1 Beoordeling van het datalek en de gevolgen.

U moet uitzoeken of er ernstige nadelige gevolgen zijn voor de bescherming van de gegevens en daarmee de persoonlijke levenssfeer van de betrokkene(n). Hierbij zijn de aard en de omvang van het datalek relevant. Het risico zal klein zijn als het bijvoorbeeld gaat om het verlies van een USB-stick met daarop enkele, niet-gevoelige persoonsgegevens. Het wordt een ander verhaal als het gaat om een 'hack' van een heel ICT-systeem, waardoor bijvoorbeeld talrijke ledenlijsten op straat komen te liggen. Als bijvoorbeeld ledenlijsten van politieke verenigingen of vakbonden of salarisadministraties zoekraken zal al snel sprake zijn van een aanmerkelijk risico voor de betrokkene, zeker gelet op de gevoeligheid van deze gegevens. U moet per incident een afweging maken naar de mate van gevoeligheid van de gelekte persoonsgegevens. Deze beoordeling is relevant voor de eventueel te maken melding van het datalek.

3.2 Is het datalek ernstig?

Er is sprake van een ernstig datalek als het gaat over bijzondere persoonsgegevens of als het lek van grote omvang is. Hieronder (zie 3.2.1) staan bijzondere persoonsgegevens genoemd.

3.2.1 Zijn er bijzondere persoonsgegevens gelekt?

Is een of meer van de onderstaande persoonsgegevens bij het datalek betrokken?

- Etnische afkomst;
- Politieke opvattingen of voorkeur;
- Religieuze opvatting of overtuiging;
- Lidmaatschap van vakbond;
- Genetische of biometrische gegevens;
- Alles op het oog op unieke identificatie (Paspoort, BSN);
- Gegevens over gezondheid;
- Gegevens over seksuele geaardheid;
- Strafrechtelijke gegevens of veroordelingen of daarmee verband houdende veiligheidsmaatregelen;
- Salarisgegevens.

3.2.2 Is het datalek van grote omvang?

Er zijn geen duidelijke regels in de wet die aangeven wanneer er sprake is van 'een grote omvang'. U moet hier zelf een inschatting maken.

3.3 Samenvatting

Is een of meer van onderstaande bijzondere persoonsgegevens bij het datalek betrokken?

- Etnische afkomst;
- Politieke opvattingen of voorkeur;
- Religieuze opvatting of overtuiging;
- Lidmaatschap van een vakbond;
- Genetische of biometrische gegevens, alles op het oog op unieke identificatie;
- Gegevens over gezondheid;
- Gegevens over seksuele geaardheid;
- Strafrechtelijke gegevens of veroordelingen of daarmee verband houdende veiligheidsmaatregelen;
- Salarisgegevens;

Schat nu zelf in of dit een datalek van een grote omvang is:

☐ Wij schatten zelf in dat dit datalek van een grote omvang is.

☐ Wij schatten zelf in dat dit datalek niet van een grote omvang is.

Geen bijzondere persoonsgegevens en geen grote omvang? Dan geen ernstig datalek!

Let op! Als er geen bijzondere persoonsgegevens zijn gelekt en het datalek is ook niet van grote omvang dan er geen sprake van een ernstig datalek. Alleen een ernstig datalek moet u melden bij de Autoriteit Persoonsgegevens.

4 Uw organisatie heeft een ernstig datalek gehad!

4.1 Melden aan de Autoriteit Persoonsgegevens!

Meld nu direct het datalek bij de Autoriteit Persoonsgegevens via onderstaande link:

https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

LET OP: U moet een datalek binnen 72 uur melden aan de Autoriteit Persoonsgegevens. Lukt dan niet binnen die 72 uur dan moet u een motivering voor de vertraging opgeven.

4.2 Melden van het datalek aan de betrokkenen?

U moet de betrokken personen informeren als de persoonsgegevens niet versleuteld waren en in de onderstaande lijst voorkomen:

- Etnische afkomst;
- Politieke opvattingen of voorkeur;
- Religieuze opvatting of overtuiging;
- Lidmaatschap van een vakbond;
- Genetische of biometrische gegevens, alles op het oog op unieke identificatie;
- Gegevens over gezondheid;
- Gegevens over seksuele geaardheid;
- Strafrechtelijke gegevens of veroordelingen of daarmee verband houdende veiligheidsmaatregelen;
- Salarisgegevens;

4.3 Wat moet u melden aan betrokkenen?

Als het nodig is om betrokkenen te informeren, dan moet u onderstaande punten in de informatie verwerken:

- Wat er gebeurd is;
- Naam en contactgegevens voor meer informatie;
- Verwachte gevolgen van het datalek voor betrokkenen;
- Wat betrokkenen nu zouden moeten doen om de schade te beperken.

4.4 Bespreek het datalek in uw organisatie.

Als u een (ernstig) datalek hebt geconstateerd, neem dan direct contact op met de directie. De directie is immers verantwoordelijk en aansprakelijk. Bespreek daarna het incident met de medewerkers en geef aan welke maatregelen u hebt genomen om herhaling te voorkomen. Het gaat hier om het herstel van vertrouwen en dat is voor elke organisatie van essentieel belang.

4.5 Samenvatting.

Ondernomen acties naar aanleiding van het geconstateerde ernstige datalek:

- ☐ Wij hebben het ernstige datalek gemeld bij de Autoriteit Persoonsgegevens.
- ☐ Wij hebben de betrokkenen geïnformeerd over het datalek.

5 Rapportage en evaluatie

5.1 Rapportage

Als u dit stappenplan datalekken hebt afgerond, sla deze rapportage zorgvuldig op en zorg ervoor dat u deze altijd kunt overleggen aan de Autoriteit Persoonsgegevens.

5.2 Evaluatie

Uw organisatie kan van een datalek veel leren. Ga met een aantal personen bij elkaar zitten en bespreek dit datalek ook aan de hand van de rapportage. Zie ook 4.4.

- ☐ Draai dit rapport uit en berg het zorgvuldig op.
- ☐ Bedenk maatregelen om nieuwe datalekken te voorkomen.

Bijlage II Standaardbrief incidenten

(Adres)

Datum	Datum
Ons kenmerk	Ons kenmerk
Contactpersoon	Naam contactpersoon
Telefoon	Telefoonnummer
E-mail	E-mailadres
Betreft	Informatie over beveiligingsincident

Geachte heer/mevrouw,

U ontvangt deze brief omdat u [cliënt of medewerker] bij ons bent of bent geweest. Wij hebben ontdekt dat een [voorbeeld: onbevoegde partij toegang heeft gehad tot onze ICT-systemen bij ons in de Organisatie]. Uit zorgvuldigheid willen wij u daarom persoonlijk hierover informeren in deze brief.

Aard van het beveiligingsincident
Wij kunnen op dit moment niet uitsluiten dat onrechtmatige verwerking van uw persoonsgegevens heeft plaatsgevonden Zoals het er nu naar uit ziet, heeft de betreffende partij toegang gehad tot [omschrijving van

het systeem/database en de functie daarvan]. Het kan hierbij gaan om de volgende gegevens [omschrijven categorieën persoonsgegevens] die zijn ingezien. [Indien er mogelijk sprake is van andere nadelige gevolgen, dan kan dat hier ook worden benoemd]

Welke maatregelen hebben wij genomen?
In reactie op het voorgevallen beveiligingsincident hebben wij de volgende stappen ondernomen: [voorbeelden]

1. Een externe specialist op het gebied van beveiliging en privacy ingeschakeld om het incident grondig te onderzoeken en aanbevelingen te doen voor verbeteringen in de beveiliging;
2. De dienst, waar het incident betrekking op heeft, hebben wij tijdelijk offline gehaald;
3. Melding gemaakt bij de Autoriteit Persoonsgegevens.

Welke preventieve maatregelen kunt u nemen? [Dit is afhankelijk van het type incident, eventueel afstemmen met de IT specialist.]
Om de eventuele negatieve gevolgen van het beveiligingsincident zoveel mogelijk te beperken raden wij u aan om zekerheidshalve de inlogcodes en wachtwoorden te wijzigen. U kunt dit doen via deze link [invoegen]. Indien u dezelfde inloggegevens en wachtwoorden voor andere diensten gebruikt, raden wij u aan om ook deze te wijzigen.

Vragen of meer informatie?
Op dit moment wordt het beveiligingsincident samen met een IT-specialist nader onderzocht. Mocht hierover meer informatie beschikbaar komen, dan zullen wij u vanzelfsprekend weer informeren.

Heeft u vragen naar aanleiding van deze brief of wilt u meer informatie ontvangen, dan kunt u ons op werkdagen tussen 08.00 en 17.00 uur bereiken op (tel. Nr.).

Wij betreuren dit voorval ten zeerste en bieden u hiervoor onze excuses aan.

Met vriendelijke groet,

G'woon Samen