



Xerio

# Privacyreglement

Versie: 2023

## Inhoudsopgave

Documentgegevens.....	3
Algemene bepalingen.....	4
1. Begripsbepalingen.....	4
2. Toepassingsgebied.....	5
3. Verantwoordelijkheden.....	5
4. Beheer van persoonsgegevens.....	5
Kenmerken van persoonsgegevens.....	5
5. Doel van de verwerking van persoonsgegevens.....	5
6. Rechtmatige grondslag gegevensverwerking.....	6
7. Opgenomen persoonsgegevens.....	7
Toegang tot en verstrekking van persoonsgegevens.....	8
8. Toegang tot persoonsgegevens.....	8
9. Verstrekking van persoonsgegevens.....	9
10. Verstrekking van persoonsgegevens aan de werkgever.....	9
Rechten van betrokkene.....	10
11. Inzage en afschrift van persoonsgegevens.....	10
12. Verbeteren, aanvullen en verwijderen van persoonsgegevens.....	11
Verplichtingen van de verantwoordelijke.....	13
13. Informatieplicht.....	13
14. Bewaren en verwijderen van persoonsgegevens.....	13
15. Beveiliging van persoonsgegevens.....	13
16. Overdracht van persoonsgegevens.....	12
Rechtsbescherming.....	14
17. Klachten.....	14
Slotbepalingen.....	14
18. Openbaarheid van dit reglement.....	14
19. Naleving van dit reglement.....	14
20. Inwerkingtreding van het reglement.....	14
Bijlage A Bewaren en verwijderen van medische gegevens.....	15



## Documentgegevens

Auteur(s)	Linda Koevoet-Ossenblok
Afdeling	Kwaliteit
Doelgroep	Medewerkers, klanten, cliënten en andere belanghebbenden van Xerio
Classificatie	Openbaar
Versie	1.3 (2021)
Status	Definitief
Datum	08-06-2021

### Versiehistorie

Versie	Opmerking
1.0	Definitieve versie
1.1	Aanpassingen data bewaartermijnen
1.2	Correcties mbt registratie en toevoeging FG
1.3	Extra aanpassingen FG
1.4	Aanpassingen FG NEN7510
1.5	Toevoeging privacy by design and privacy by default

## Contactgegevens

Xerio B.V.

Gastelseweg 142 D-E

4705 RB Roosendaal

[info@xerio.nl](mailto:info@xerio.nl)

0165-522010

Contactpersoon: Arjan Vermeulen

Functionaris Gegevensbescherming: Maarten de Man



## Algemene bepalingen

Xerio verwerkt in het kader van haar bedrijfsvoering persoonsgegevens en vindt het belangrijk dat met persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld. De Algemene Verordening Gegevensbescherming beoogt waarborgen te verschaffen ter bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Dit privacyreglement beoogt:

- Richtlijnen te geven aan Xerio voor de omgang met persoonsgegevens;
- Informatie te verschaffen aan personen van wie persoonsgegevens door Xerio verwerkt (zullen) worden.

### 1. Begripsbepalingen

- 1.1. *De wet*: het wettelijk kader voor privacybescherming waaronder de Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene Verordening Gegevensbescherming;
- 1.2. *Het reglement*: Dit reglement, inclusief de bijlagen;
- 1.3. *Persoonsgegeven*: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
- 1.4. *Gezondheidsgegevens*: persoonsgegevens die direct of indirect betrekking hebben op de lichamelijke of de geestelijke gesteldheid van betrokkenen;
- 1.5. *Verwerking van persoonsgegevens*: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
- 1.6. *Verstrekken van persoonsgegevens*: het bekendmaken of ter beschikking stellen van persoonsgegevens die in de registratie(s) zijn opgenomen of die door verwerking daarvan, al dan niet in verband met andere gegevens, zijn verkregen;
- 1.7. *Verzamelen van persoonsgegevens*: het verkrijgen van persoonsgegevens;
- 1.8. *Bestand*: elk samenhangend geheel van persoonsgegevens, ongeacht of dit geheel van gegevens bij elkaar of gescheiden van elkaar wordt verzameld, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
- 1.9. *Verantwoordelijke*: de natuurlijke persoon, rechtspersoon of ieder ander die alleen, of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
- 1.10. *Personeel*: personen in dienst van of werkzaam ten behoeve van de verantwoordelijke;
- 1.11. *Verwerker*: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
- 1.12. *Gebruiker*: enig persoon die, onder gezag van de verantwoordelijke, gemachtigd is persoonsgegevens te verwerken, dan wel van enigerlei uitvoer van de verwerking kennis te nemen;

- 1.13. *Beheerder*: degene die ten behoeve van de verantwoordelijke is belast met de dagelijkse zorg voor het beheer van de gegevensverwerking;
- 1.14. *Betrokkene*: degene op wie een persoonsgegeven betrekking heeft;
- 1.15. *Werkgever*: iedere rechtspersoon die een overeenkomst heeft gesloten met verantwoordelijke en wederpartij is in de arbeidsverhouding met de betrokkene;
- 1.16. *Derde*: ieder ander dan de betrokkene, de verantwoordelijke, de gebruiker of de verwerker;
- 1.17. *Ontvanger*: degene aan wie persoonsgegevens worden verstrekt;
- 1.18. *Toestemming van de betrokkene*: elke vrije, specifieke en op adequate informatie berustende wilsuiting van de betrokkene waarmee deze aanvaardt dat op hem/haar betrekking hebbende persoonsgegevens worden verwerkt;

## 2. Toepassingsgebied

- 2.1. Dit reglement is van toepassing op elke, al dan niet (gedeeltelijk) geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin opgenomen te worden.
- 2.2. Dit reglement is van toepassing binnen Xerio en heeft betrekking op de verwerking van persoonsgegevens van klanten, cliënten. Verwerking van persoonsgegevens van de medewerkers van Xerio valt buiten de reikwijdte van dit reglement.

## 3. Verantwoordelijkheden

- 3.1. Xerio is verantwoordelijk voor het bepalen van het doel, de inhoud en het gebruik van de verwerking van persoonsgegevens en voor de naleving van de bepalingen in dit reglement.
- 3.2. Dit reglement komt tot stand en wordt beheerd onder verantwoordelijkheid van de verantwoordelijke, te weten de directie van Xerio B.V.

## 4. Beheer van persoonsgegevens

- 4.1. In het kader van de verwerking van persoonsgegevens sluit de verantwoordelijke aan bij de toepasselijke wet- en regelgeving op het gebied van privacy en informatiebeveiliging, richtlijnen van de brancheorganisatie arbodiensten OVAL en de (overkoepelende) beroepsorganisaties KNMG en NVAB, alsmede bij de eisen die de certificerende instelling aan haar stelt.
- 4.2. De persoonsgegevens worden in opdracht van de verantwoordelijke verwerkt door een verwerker. In de daartoe opgestelde verwerkersovereenkomst is vastgelegd dat de verwerker de persoonsgegevens slechts verwerkt ten behoeve van de verantwoordelijke, overeenkomstig diens instructies en onder diens verantwoordelijkheid een en ander met inachtneming van onderhavig reglement.

## Kenmerken van persoonsgegevens

### 5. Doel van de verwerking van persoonsgegevens

- 5.1. De verantwoordelijke verwerkt persoonsgegevens in het kader van de dienstverlening aan klanten op het gebied van integraal gezondheidsmanagement, arbeidsomstandigheden,

verzuimbegeleiding, re-integratie, interventies, preventie, gezondheidsonderzoeken, keuringen, coachingstrajecten, trainingen, vaccinaties, overige contractuele afspraken en financiële afhandelingen van eerder genoemde diensten.

- 5.2. De persoonsgegevens moeten toereikend zijn, ter zake dienend en niet bovenmatig gelet op de doeleinden waarvoor de persoonsgegevens worden verzameld of verwerkt. Verantwoordelijke zal niet meer gegevens in de registratie opslaan of bewaren dan voor het in 5.1 genoemde doel noodzakelijk is.
- 5.3. Indien de verantwoordelijke persoonsgegevens voor andere doeleinden dan genoemd in 5.1 wenst te verwerken, heeft de verantwoordelijke de plicht de betrokkene vooraf gericht te informeren omtrent de aard van de gegevens die over zijn persoon in de verwerking worden opgenomen, alsmede omtrent de doeleinden die daarmee worden nagestreefd. Deze verplichting geldt niet wanneer persoonsgegevens niet (meer) tot individuele natuurlijke personen te herleiden zijn.
- 5.4. Persoonsgegevens kunnen afkomstig zijn van de betrokkene zelf, diens leidinggevende of werkgever, personeel van de verantwoordelijke, externe professionals en beroepsbeoefenaars, het UWV of andere bij de dienstverlening betrokken derden.

## 6. Rechtmatige grondslag gegevensverwerking

- 6.1. Op grond van de Algemene Verordening Gegevensbescherming dient er voor iedere verwerking van persoonsgegevens een rechtmatige grondslag te zijn. Deze grondslag is aanwezig indien:
  - 6.1.1. Er sprake is van ondubbelzinnige toestemming van de betrokkene;
  - 6.1.2. De gegevensverwerking noodzakelijk is:
    - Voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
    - Voor het nakomen van een wettelijke verplichting waaraan de verantwoordelijke is onderworpen;
    - Ter vrijwaring van een vitaal belang van betrokkene (denk aan een dringende medische oorzaak, zoals verlies van het bewustzijn);
    - Voor de goede vervulling van een publiekrechtelijke taak door het bestuursorgaan;
    - Voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke of van een derde waaraan de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden de betrokkene prevaleren.
- 6.2. De verwerking van persoonsgegevens door de verantwoordelijke voldoet steeds aan één van de in 6.1 genoemde grondslagen. In de meeste gevallen zal dit gaan om de uitvoering van de afgesloten overeenkomst (het basiscontract) met de werkgever.
- 6.3. Persoonsgegevens worden in overeenstemming met dit reglement op behoorlijke en zorgvuldige wijze verwerkt. In dit kader treft de verantwoordelijke de nodige maatregelen om de integriteit en beschikbaarheid van de persoonsgegevens te waarborgen en draagt zorg voor de beveiliging van de persoonsgegevens tegen verlies af aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan. Gelijke plicht rust op de verwerker voor het geheel of het gedeelte van de faciliteiten, die hij onder zich heeft.
- 6.4. De te verwerken persoonsgegevens worden slechts verder verwerkt op een wijze die niet onverenigbaar is met het doel waarvoor ze zijn verkregen. Daarbij wordt ten minste rekening gehouden met de verwantschap van de doelen, de aard van de gegevens, de

gevolgen van de verdere verwerking voor de betrokkene, de wijze waarop de gegevens zijn verkregen en de waarborgen ter bescherming van de persoonlijke levenssfeer.

Persoonsgegevens mogen verder worden verwerkt wanneer dat noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is of geschiedt met de ondubbelzinnige toestemming van de betrokkene.

- 6.5. De gegevens worden alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een (arbeids)overeenkomst tot geheimhouding zijn verplicht.
- 6.6. De verantwoordelijke bewaart geheimhouding over de persoonsgegevens waarvan hij/zij kennisneemt, behoudens voor zover enig wettelijk voorschrift hem/haar tot mededeling verplicht of uit zijn/haar taak mededeling voortvloeit.
- 6.7. De verantwoordelijke verwerkt geen persoonsgegevens betreffende iemand godsdienst of levensovertuiging, ras, politieke gezindheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging.
- 6.8. Artikel 6.7 is niet van toepassing voor zover:
  - Dit noodzakelijk is in aanvulling op de verwerking van persoonsgegevens betreffende iemands gezondheid met het oog op een goede behandeling of begeleiding van betrokkene;
  - Dit geschiedt met schriftelijke toestemming van betrokkene;
  - De gegevens door betrokkene openbaar zijn gemaakt en hierbij toestemming is gegeven voor verdere verwerking;
  - Dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte;
  - Dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende maatregelen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel de AP ontheffing heeft verleend. De AP kan bij de verlening van ontheffing beperkingen en voorschriften opleggen.
- 6.9. Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.
- 6.10. Vastlegging en verstrekking van (medische) persoonsgegevens gebeurt op basis van de KNMG-code.
- 6.11. Bij het printen of anderszins exporteren of verstrekken van medische gegevens wordt medische informatie als zodanig gelabeld.

## 7. Opgenomen persoonsgegevens

- 7.1. Persoonsgegevens, die door de verantwoordelijke worden verwerkt, zijn verzameld door de medewerkers van de verantwoordelijke en verstrekt door de betrokkene, de werkgever van de betrokkene, het UWV of door eventuele behandelaar(s) van de betrokkene of andere bij de dienstverlening betrokken derden.
- 7.2. Bij de inrichting van procedures, procedures en formulieren past Xerio de principes van privacy by design en privacy by default toe.
- 7.3. De navolgende persoonsgegevens kunnen door de verantwoordelijke met inachtneming van het bepaalde in dit reglement worden verwerkt:
  - naam en geboortedatum;
  - adres, plaats en telefoonnummer van zowel de woonplaats als een tijdelijke verblijfplaats;

- geslacht, burgerlijke staat, geboorteland, nationaliteit;
- bedrijf / instelling, afdeling, functie, aard dienstverband, datum in- en uitdiensttreding;
- personeelsnummer, Burgerservicenummer (slechts bij gegevensuitwisseling UWV);
- naam, adres, woonplaats en telefoonnummer van huisarts en overige behandelaars;
- arbeidsomstandigheden;
- resultaten van incidentele en periodieke gezondheidsonderzoeken;
- gegevens voortvloeiende uit het spreekuur;
- gegevens voortvloeiende uit de ziekmelding door de werkgever en de daarop aansluitende eigen verklaring;
- gegevens voortvloeiend uit huisbezoek;
- de belastbaarheid in relatie tot de belasting in het werk;
- voorgestelde en getroffen re-integratiemaatregelen en aanpassingen in de arbeidsomstandigheden;
- overige gegevens nodig t.b.v. de re-integratie (waaronder de re-integratiemogelijkheden);
- resultaten van overleg met de werkgever, behandelaars, uitvoeringsinstellingen voor de sociale zekerheid en verzekeringsmaatschappijen.

## Toegang tot en verstrekking van persoonsgegevens

### 8. Toegang tot persoonsgegevens

- 8.1. Onverminderd eventuele wettelijke voorschriften ter zake hebben slechts toegang tot persoonsgegevens de beroepsbeoefenaar die deze gegevens heeft verzameld of diens waarnemer, alsmede degenen die rechtstreeks betrokken zijn bij de behandeling of bedrijfsgeneeskundige begeleiding van de betrokkene.
- 8.2. De beheerder en de verwerker hebben toegang tot persoonsgegevens voor zover dit in het kader van de uitoefening van hun taken noodzakelijk is.
- 8.3. Onder verantwoordelijkheid van de beheerder kunnen externe personen worden ingeschakeld ten behoeve van technisch onderhoud aan en/of aanpassing van de systemen van de verantwoordelijke. Deze personen verkrijgen toegang tot persoonsgegevens voor zover dit voor de uitvoering van hun werkzaamheden noodzakelijk is.
- 8.4. De personen, bedoeld in de artikelen 8.1, 8.2 en 8.3, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens, waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of hun taak de noodzaak tot mededeling voortvloeit. Hiertoe ondertekenen zij een geheimhoudingsverklaring.
- 8.5. De personen, genoemd in artikel 8.1, zijn ieder voor zich verantwoordelijk voor een juiste en zorgvuldige vastlegging en raadpleging van de persoonsgegevens. De beroepsbeoefenaars zijn daarnaast verantwoordelijk voor het dossier dat zij in verband met hun taakuitoefening aanleggen.
- 8.6. Middels een rechtenstructuur in de software hebben uitsluitend daartoe geautoriseerde personen toegang tot persoonsgegevens. Autorisatie vindt plaats aan de hand van de door de verantwoordelijke vastgestelde functies en bijbehorende rechten en rollen. Indien hiervan wordt afgeweken, wordt dit door de verantwoordelijke op klantniveau geregistreerd.



8.7 De verantwoordelijke heeft als zodanig geen toegang tot persoonsgegevens, tenzij dit noodzakelijk is in verband met zijn algemene verantwoordelijkheid als verantwoordelijke.

## 9. Verstrekking van persoonsgegevens

9.1 Met inachtneming van het bij of krachtens de Algemene Verordening Gegevensbescherming en de regels voor de verwerking van persoonsgegevens van zieke werknemers van de AP ("De zieke werknemer en privacy", februari 2008) bepaalde worden persoonsgegevens zonder voorafgaande toestemming van de betrokkene verstrekt aan:

- a) medewerkers van de verantwoordelijke die direct betrokken zijn bij de actuele dienstverlening aan en begeleiding van betrokkene (als genoemd in artikel 8.1);
- b) verwerkers van persoonsgegevens in het kader van de gegeven opdracht door de verantwoordelijke, mits deze verwerkers voldoende waarborgen bieden dat de bescherming van de persoonsgegevens plaatsvindt overeenkomstig alle artikelen van dit reglement;
- c) instituten ten behoeve van wetenschappelijke of statistische doelen indien en voor zover deze persoonsgegevens geanonimiseerd zijn (dat wil zeggen niet meer herleidbaar tot betrokkenen); en hierbij voldaan is aan de eisen van de AP ten aanzien van anonimisering/ pseudonimisering
- d) de betrokkene zelf;
- e) de werkgever van de betrokkene in geval van verzuimbegeleiding, mits het slechts de volgende gegevens betreft:
  - naam en geboortedatum,
  - datum van het laatste consult,
  - conclusies ten aanzien van de mogelijkheden tot werkhervatting door de betrokkene,
  - procesmatige begeleidingsafspraken;
- f) uitvoeringsinstituten voor de sociale verzekeringen in het kader van het re-integratieplan volgens de richtlijnen van het UWV;
- g) verzekeringsmaatschappijen in het kader van de verzekering van de loondoorbetaling bij ziekte volgens het Convenant gegevensuitwisseling arbodiensten - verzekeraars.
- h) het Nederlands Centrum voor Beroepsziekten, op basis van de wettelijke verplichting van melding door arbodiensten, ten behoeve van wetenschappelijke of statistische doelen, mits deze gegevens de betrokkene niet identificeren.

9.2. Andere gegevens en gegevens aan anderen dan genoemd in artikel 9.1 worden slechts verstrekt na gerichte toestemming van de betrokkene. Van de toestemming wordt aantekening gemaakt in het medisch dossier of de betrokkene tekent een daartoe specifiek opgestelde machtiging, welke wordt opgeslagen in het dossier van de arbodienst.

9.3. Er worden geen persoonsgegevens doorgegeven buiten de EU of aan een internationale organisatie, anders dan de werkgever.

## 10. Verstrekking van persoonsgegevens aan de werkgever

10.1 Op informatie die is verzameld in het kader van vrijwillig aangegane contacten, is de Wet Geneeskundige Behandelingsovereenkomst (WGBO) integraal van toepassing. Dit betekent dat de arbo- en gezondheidsdienst slechts met uitdrukkelijke toestemming van de betrokkene persoonsgegevens aan de werkgever mag verstrekken.

10.2 In aanvulling op artikel 10.1 geldt dat aan de werkgever geen mededelingen zullen worden gedaan over bezoek aan het arbeidsomstandighedenspreekuur door betrokkene. Ook de vrijwillige deelname aan een PAGO/PMO geschiedt anoniem, tenzij betrokkene voorafgaand aan het gezondheidsonderzoek is gewezen op het feit dat zijn deelname bekend is/wordt gemaakt bij de werkgever en betrokkene hiermee heeft ingestemd. Indien de arbo- en gezondheidsdienst naar aanleiding van het arbeidsomstandighedenspreekuur of het gezondheidsonderzoek advies richting de werkgever wenst uit te brengen, is daarvoor de uitdrukkelijke toestemming van betrokkene nodig. Van de toestemming wordt aantekening gemaakt in het medisch dossier of de betrokkene tekent een daartoe specifiek opgestelde machtiging, welke wordt opgeslagen in het dossier van de arbo- en gezondheidsdienst.

10.3 In het kader van de dienstverlening op het gebied van verzuimbegeleiding en re-integratie, is het de arbo- en gezondheidsdienst toegestaan om die informatie aan de werkgever terug te koppelen die noodzakelijk is voor de werkgever om te bepalen of er sprake is van legitiem verzuim in het kader van de loondoorbetaling, alsook die informatie die noodzakelijk is in het kader van verzuimbegeleiding en re-integratie op basis van onder meer de Wet Verbetering Poortwachter. Meer specifiek ontvangt de werkgever slechts gerichte informatie over:

- functionele beperkingen, restmogelijkheden en implicaties voor het soort arbeid dat de betrokkene nog kan verrichten;
- de werkzaamheden waartoe de betrokkene nog wel, of juist niet meer in staat is;
- het verwachte einddoel van de re-integratie (geschiktheid voor eigen werk, passend werk of re-integratie tweede spoor) met zo mogelijk een indicatie van de verwachte duur van het verzuim;
- de eventuele aanpassingen, werkvoorzieningen of activiteiten die de betrokkene en de werkgever in het kader van de re-integratie moeten treffen.

De betrokkene wordt voorafgaand aan de informatieverstrekking aan de werkgever geïnformeerd over de inhoud daarvan. In het kwaliteitsmanagementsysteem van de verantwoordelijke is nader gespecificeerd wat wel en wat niet aan de werkgever gerapporteerd mag worden.

10.4 In aanvulling op artikel 10.3 geldt dat aan de werkgever geen medische gegevens worden verstrekt, tenzij dit naar de mening van de beroepsbeoefenaar noodzakelijk is en de betrokkene hiervoor zijn uitdrukkelijke toestemming heeft gegeven. Van de toestemming wordt aantekening gemaakt in het medisch dossier of de betrokkene tekent een daartoe specifiek opgestelde machtiging, welke wordt opgeslagen in het dossier van de arbo- en gezondheidsdienst.

10.5 Verzuimoverzichten of groepsrapportages voor een werkgever of diens medezeggenschapsorgaan bevatten geen persoonsgegevens die herleidbaar zijn tot individuele personen.

## Rechten van betrokkene

### 11. Inzage en afschrift van persoonsgegevens

11.1 De verantwoordelijke deelt een ieder op diens verzoek, zo spoedig mogelijk maar uiterlijk binnen een maand na ontvangst van het verzoek, schriftelijk mee of hem betreffende persoonsgegevens worden verwerkt. Indien dit inderdaad het geval is, zendt de verantwoordelijke tevens een overzicht van de betreffende gegevens mee.

- 11.2 De gevraagde kennisneming wordt aan de betrokkene in persoon verleend, door het tonen van de op deze persoon betrekking hebbende gegevens. De betrokkene dient zich vooraf te legitimeren.
- 11.3 De betrokkene heeft recht op kopieën van de in artikel 7.2 bedoelde gegevens. Voor de verstrekking hiervan mag een redelijke vergoeding in rekening worden gebracht.
- 11.4 Een verzoek tot kennisneming kan met redenen omkleed worden geweigerd, evenals het verstrekken van kopieën.
- 11.5 Kennisneming is eveneens mogelijk door een daartoe schriftelijk gemachtigde (vertrouwens)persoon van de betrokkene. De machtiging moet voldoende specifiek aangeven op welke gegevens het verzoek om kennisneming en/of afschrift ziet.

## 12. Recht op rectificatie en aanvulling van persoonsgegevens

- 12.1 Op schriftelijk verzoek van de betrokkene of diens gevolmachtigde gaat de verantwoordelijke over tot het verbeteren, aanvullen of verwijderen van de persoonsgegevens die op de betrokkene betrekking hebben, indien en voor zover deze gegevens feitelijk onjuist zijn, voor het doel van de verwerking onvolledig, niet ter zake dienend of bovenmatig zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen en de motivatie hiervoor.
- 12.2 De verantwoordelijke deelt de betrokkene zo spoedig mogelijk maar uiterlijk binnen een maand na ontvangst van het verzoek schriftelijk mee of hij daaraan voldoet. Hieraan ligt een gemotiveerde beslissing ten grondslag.
- 12.3 De verantwoordelijke draagt ervoor zorg dat een beslissing tot verbetering of aanvulling van persoonsgegevens zo spoedig mogelijk wordt uitgevoerd, doch uiterlijk binnen drie maanden na de datum waarop de beslissing aan de betrokkene is gecommuniceerd.
- 12.4 Een verzoek tot verwijdering van persoonsgegevens wordt niet ingewilligd wanneer redelijkerwijs aannemelijk is dat bewaring een aanmerkelijk belang dient voor een ander dan de betrokkene, alsmede wanneer bewaring op grond van een wettelijk voorschrift is vereist.

## 13. Recht op vergetelheid van persoonsgegevens

- 13.1 Op schriftelijk verzoek van de betrokkene of diens gevolmachtigde gaat de verantwoordelijke over tot het wissen van de persoonsgegevens die op de betrokkene betrekking hebben, indien en voor zover deze gegevens niet meer nodig zijn, de betrokkene uitdrukkelijk gegeven toestemming intrekt, bezwaar maakt waarbij de rechten van betrokkene zwaarder wegen dan het belang van de organisatie om persoonsgegevens te verwerken, er sprake is van onrechtmatige verwerking, de geldende bewaartermijn is verstreken of er sprake is betrokkenen van jonger dan 16 jaar waarbij de gegevens zijn verzameld via een app of website.
- 13.2 De verantwoordelijke draagt er zorg voor dat de gegevens binnen één maand na de aanvraag gewist worden. In complexe situaties mogen zij hiervoor twee maanden de tijd nemen, maar laten dan uiterlijk binnen één maand aan betrokkene weten dat het twee maanden gaat duren.
- 13.3 Een verzoek tot vergetelheid brengt in principe geen kosten met zich mee. Als een verzoek ongegrond of buitensporig is, is de verantwoordelijke gerechtigd een administratieve vergoeding in rekening te brengen.

## 14. Recht op dataportabiliteit van persoonsgegevens

14.1 De betrokkene heeft het recht op hem betrekking hebbende persoonsgegevens te doen overdragen aan een andere, door hem aan te wijzen, verantwoordelijke. Dit komt voor als de werkgever van betrokkene bijvoorbeeld verandert van arbodienst c.q. de arbeidsomstandighedenwet. De betrokkene dient voor de overdracht van zijn persoonsgegevens een schriftelijk verzoek in bij de verantwoordelijke. De inwilliging van dit verzoek kan slechts worden geweigerd op grond van een wettelijk voorschrift dan wel worden opgeschort voor zover de verantwoordelijke jegens de financier van verleende zorg tot bewaring gehouden is of indien ter zake van die zorg een geschil aanhangig is gemaakt of dreigt te worden gemaakt.

14.2 Voor het overdragen van de persoonsgegevens van de betrokkene naar een andere verantwoordelijke mag een redelijke vergoeding in rekening worden gebracht.

14.3 In geval de verantwoordelijke het voornemen heeft tot overdracht van door haar gehouden persoonsgegevens, bijvoorbeeld in verband met beëindiging van de onderneming, worden de betrokkenen door middel van een openbare bekendmaking in kennis gesteld van dit voornemen. De betrokkenen die op het moment van bekendmaking onder behandeling zijn, worden hiervan persoonlijk in kennis gesteld. In deze bekendmaking worden de reden(en) van de overdracht en de beoogde nieuwe verantwoordelijke vermeld. Binnen twee maanden na de bekendmaking kan tegen de overdracht bezwaar worden gemaakt. Indien tegen de overdracht bezwaar wordt gemaakt, stelt de verantwoordelijke in overleg met de betrokkene vast wat er met de gegevens gebeurt. Indien wordt geopteerd voor vernietiging van de gegevens, dient dit binnen drie maanden kosteloos te geschieden. Wanneer de persoonsgegevens worden overgedragen naar een andere verantwoordelijke blijven de in dit reglement gestelde regels van toepassing.

## 15. Recht op beperking van de verwerking van persoonsgegevens

15.1 In de volgende situaties heeft de betrokkene het recht op een beperking van de verwerking van de gegevens:

- a) Gegevens zijn mogelijk onjuist: indien wordt aangegeven dat gegevens mogelijk onjuist zijn, moet de verantwoordelijke deze gegevens eerst controleren, alvorens ze te gebruiken.
- b) De verwerking is onrechtmatig: de verwerking van gegevens is onrechtmatig, maar betrokkene wil niet dat u de gegevens wist.
- c) Gegevens zijn niet meer nodig: gegevens zijn niet meer nodig voor uw verwerking, maar de betrokkene heeft de gegevens nog wel nodig voor een rechtsvordering.
- d) Betrokkene maakt bezwaar: zolang er nog geen uitspraak is geweest, mag de verantwoordelijke niet verder gaan met de verwerking van de gegevens.

## 16. Recht op bezwaar

16.1 Betrokkenen hebben recht om bezwaar te maken tegen verwerking van persoonsgegevens als de organisatie gegevens verwerkt op grond van een taak van algemeen belang of op grond van gerechtvaardigd belang. Verantwoordelijke verwerkt geen gegevens op deze grondslagen. Betrokkenen kunnen dus geen bezwaar indienen.

## Verplichtingen van de verantwoordelijke

### 17. Informatieplicht

- 17.1 Indien de verantwoordelijke de persoonsgegevens verkrijgt bij de betrokkene zelf, deelt de verantwoordelijke voor of op het moment van verkrijging zijn identiteit mee alsmede het doel van de verwerking waarvoor de persoonsgegevens zijn bestemd, tenzij de betrokkene hiervan reeds op de hoogte is.

### 18. Bewaren en verwijderen van persoonsgegevens

- 18.1 Met inachtneming van eventuele wettelijke voorschriften en de doeleinden waarvoor de gegevens worden verwerkt, stelt de verantwoordelijke de bewaartermijn van de persoonsgegevens vast.
- 18.2 Ten aanzien van persoonsgegevens die worden aangemerkt als medische gegevens gelden de bewaartermijnen zoals neergelegd in Bijlage A. Deze bijlage wordt geacht één geheel te vormen met dit reglement.
- 18.3 Wanneer de door de verantwoordelijke vastgestelde bewaartermijn is verstreken, worden de persoonsgegevens binnen één jaar verwijderd.
- 18.4 Het verwijderen blijft eventueel achterwege wanneer redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, alsmede bewaring op grond van een wettelijk voorschrift vereist is of indien daarover tussen de betrokkene en de beroepsbeoefenaar overeenstemming bestaat. Indien de betreffende gegevens zodanig zijn bewerkt dat herleiding tot identificeerbare personen redelijkerwijs onmogelijk is, kunnen zij in deze geanonimiseerde vorm bewaard blijven.

### 19. Beveiliging van persoonsgegevens

- 19.1 De verantwoordelijke neemt passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, zodat de vertrouwelijkheid, integriteit en beschikbaarheid van de persoonsgegevens wordt gewaarborgd.
- 19.2 De verantwoordelijke heeft de beveiliging van persoonsgegevens onder meer geregeld in een separaat informatiebeveiligingsplan. Dit informatiebeveiligingsplan is gebaseerd op de NEN7510. In dit informatiebeveiligingsplan wordt bijvoorbeeld aandacht besteed aan:
- beveiliging van de toegang tot de geautomatiseerde omgeving;
  - fysieke beveiliging van datacentra en kantoren;
  - screening van het personeel en het hanteren van gedragscodes omtrent het omgaan met vertrouwelijke informatie;
  - bedrijfscontinuïteit bij calamiteiten;
  - het verzorgen van back-ups;
- 19.3 Digitale gegevens worden in beginsel opgeslagen in informatiesystemen van de verantwoordelijke of van de verwerker. Papieren gegevens worden opgeslagen in afgesloten kasten en bureaus op locaties van Xerio.
- 19.4 De medewerkers die in dienst zijn bij de arbo- en gezondheidsdienst als ook derden die worden ingeschakeld ten behoeve van de dienstverlening aan klanten tekenen een geheimhoudingsverklaring.
- 19.5 De verantwoordelijke conformeert zich aan de meldplicht datalekken zoals deze in de beleidsregels van de meldplicht zijn beschreven. Er is een interne procedure aanwezig voor



het afhandelen van incidenten. De verantwoordelijke treft maatregelen om de AP en betrokkenen te informeren indien dit in het kader van de meldplicht aan de orde is.

## Rechtsbescherming

### 20. Klachten

- 20.1 Indien de betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd en/of de verantwoordelijke de rechten van betrokkene met betrekking tot de verwerking van persoonsgegevens niet respecteert, dient betrokkene zich met zijn klacht te wenden tot de verantwoordelijke. De verantwoordelijke zal vervolgens de klacht afhandelen conform de klachtenregeling zoals opgenomen in het kwaliteitsmanagementsysteem van de verantwoordelijke.
- 20.2 Indien de klachtafhandeling door de verantwoordelijke voor de betrokkene niet leidt tot een voor hem acceptabel resultaat, heeft de betrokkene de mogelijkheid om een klacht in te dienen bij de Geschillencommissie Arbodiensten of de Autoriteit Persoonsgegevens. Tot slot kan betrokkene zich ook tot de rechtbank wenden met het schriftelijk verzoek om de verantwoordelijke te bevelen (alsnog) aan bepaalde verplichtingen uit de Algemene Verordening Gegevensbescherming te voldoen.

### 21. Functionaris Gegevensbescherming

- 21.1 Xerio heeft een functionaris gegevensbescherming aangesteld binnen haar organisatie. Iedere betrokkene kan zich direct tot de functionaris gegevensbescherming wenden door te mailen naar: [deman@avgjuristen.nl](mailto:deman@avgjuristen.nl).

## Slotbepalingen

### 22. Openbaarheid van dit reglement

Het reglement is in te zien en gratis te downloaden via de website [www.xerio.nl](http://www.xerio.nl). Op verzoek wordt eveneens kosteloos een papieren exemplaar van dit reglement ter beschikking gesteld.

### 23. Naleving van dit reglement

- 22.1 Via periodieke interne audits wordt door de verantwoordelijke onderzoek gedaan naar naleving van de bepalingen uit onderhavig reglement.
- 22.2 De naleving van dit reglement wordt getoetst door de certificerende instelling door middel van jaarlijkse externe audits.

### 24. Inwerkingtreding van dit reglement

De verantwoordelijke hanteert sinds 1 november 2017 onderhavig reglement. Dit reglement wordt door de verantwoordelijke geactualiseerd indien nodig. De laatste revisie van het reglement is steeds van toepassing.



## Bijlage A Bewaren en verwijderen van medische gegevens

De verantwoordelijke conformeert zich aan de algemene richtlijnen voor het bewaren en verwijderen van medische gegevens van de Koninklijke Nederlandse Maatschappij ter bevordering der Geneeskunst (KNMG), welke richtlijnen bij de verantwoordelijke kunnen worden ingezien of opgevraagd.

Met inachtneming van de KNMG-richtlijnen inzake het bewaren en verwijderen van medische gegevens gelden de volgende uitgangspunten:

- a. Na het overlijden van de betrokkene worden de persoonsgegevens na een bewaartermijn van 20 jaar en indien blootstelling aan carcinogene stoffen of biologische agentia heeft plaatsgevonden 40 jaar en bij werken met ioniserende straling 30 jaar, binnen één jaar verwijderd.
- b. Bij beëindiging van de arbodienst worden de persoonsgegevens na een bewaartermijn van 20 jaar en indien blootstelling aan carcinogene stoffen of biologische agentia heeft plaatsgevonden 40 jaar en bij werken met ioniserende straling 30 jaar, binnen één jaar verwijderd.
- c. Na uit dienst treden bij de werkgever, waar de betrokkene werkzaam is, of na beëindiging van het contract van de werkgever met de arbo- en gezondheidsdienst worden de persoonsgegevens op verzoek van betrokkene dan wel met diens instemming overgedragen aan de nieuwe verantwoordelijke of anders, na een bewaartermijn van 20 jaar en indien blootstelling aan carcinogene stoffen of biologische agentia heeft plaatsgevonden 40 jaar en bij werken met ioniserende straling 30 jaar, binnen één jaar verwijderd.
- d. De verantwoordelijke bewaart de medische gegevens in afwijking van het bepaalde onder sub a t/m c zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.
- e. Door het gebruik van back-ups behoudt de verantwoordelijke zich het recht de gegevens in een back-up aanvullend 1 jaar te bewaren.