Privacybeleid

Datum: 01-05-2018

A. ALGEMEEN

A.1. DOEL VAN DIT PRIVACYBELEID
Dit privacy-beleid is bedoeld om een algemeen "raamwerk" te omschrijven voor hoe It Fits Human Protection met persoonsgegevens omgaat. Voor meer specifieke verwerkingen van persoonsgegevens binnen de organisatie van It Fits Human Protection kunnen specifiekere regelingen (zoals protocollen) gelden.

A.2. "SCOPE" VAN DIT PRIVACYBELEID
De omvang (of "scope") van dit privacy-beleid strekt zich uit over It Fits Human Protection en de persoonsgegevens waarvoor It Fits Human Protection is aan te merken als verantwoordelijke.
Het gaat daarbij o.a. om de volgende soorten persoonsgegevens:
• Persoonsgegevens van werknemers
• Persoonsgegevens van patiënten
• Persoonsgegevens van cliënten

A.3. GEBRUIKTE BEGRIPPEN
In bijlage 1 bij dit document zijn de relevante begrippen uit de privacy wetgeving omschreven die in dit privacy-beleid worden gebruikt.

B. WETTELIJK KADER

B.1. ALGEMENE VERORDENING GEGEVENSBESCHERMING
Op het gebruik ("verwerken") van persoonsgegevens door It Fits Human Protection is per 25 mei 2018 de Algemene Verordening Gegevensbescherming van toepassing. Vanaf die dag vervangt de AVG de Nederlandse Wet bescherming persoonsgegevens ("Wbp"). De AVG is van toepassing op :

• het "geautomatiseerd" verwerken van persoonsgegevens, "geautomatiseerd" is kort gezegd het verwerken via een computer of ander elektronisch apparaat zoals een smartphone, tablet, digitale camera of via een server. Veel voorkomende voorbeelden zijn het aanleggen van klantendatabases, het verzenden en ontvangen van e-mails, het verzamelen van gegevens via een website of een app, het maken van cameraopnamen, het vastleggen van gegevens van werknemers vastleggen; en
• het op papier verwerken van persoonsgegevens in een "geordend geheel" (in een doorzoekbaar bestand).

Een voorbeeld van dit laatste is de fysieke mappenadministratie van personeelsdossiers.
It Fits Human Protection heeft op grond van de AVG als "verantwoordelijke" bepaalde verplichtingen rond het verwerken van de persoonsgegevens. De personen om wiens gegevens het gaat (de "betrokkenen") hebben op grond van de AVG bepaalde rechten wat betreft het verwerken van hun persoonsgegevens. In dit beleid wordt in algemene bewoordingen omschreven wat die verplichtingen en rechten zijn.

B.2. ANDERE SPECIFIEKE WET- EN REGELGEVING
In bepaalde specifieke situaties, zoals voor het gebruik van persoonsgegevens van werknemers, medische gegevens of strafrechtelijke persoonsgegevens kan aanvullende wet- en regelgeving gelden.

C. BASISBEGINSELEN

C.1. ALGEMEEN
In het algemeen geldt dat "zorgvuldig" met persoonsgegevens moet worden omgegaan. Medewerkers van It Fits Human Protection moeten zich daarom, bij het gebruiken van persoonsgegevens tijdens hun dagelijkse werkzaamheden, bedenken dat de privacyregels van de AVG in acht worden genomen.

C.2. VERZAMELEN, ONTVANGEN EN INTERN GEBRUIKEN VAN PERSOONSGEGEVENS
Bij het verzamelen/creëren van persoonsgegevens, het ontvangen van persoonsgegevens van externe partijen en het verder intern verwerken daarvan binnen It Fits Human Protection , wordt door It Fits Human Protection een afweging gemaakt of dat mag, en zo ja, hoe ver het gebruik kan gaan.
Daarbij wordt minimaal rekening gehouden met de volgende vragen (in Bijlage 1 staan de gebruikte begrippen uitgelegd):
• Gaat het om "bijzondere persoonsgegevens"? Dan mogen deze alleen worden verzameld, ontvangen en verwerkt op basis van een wettelijke uitzondering. Als de bijzondere persoonsgegevens mogen worden verwerkt, geldt dat extra voorzichtig met deze persoonsgegevens moet worden omgegaan.
• Gaat het om persoonsgegevens van kinderen (personen onder de 16 jaar)? Dan moet ook extra voorzichtig met de gegevens worden omgegaan en gelden er extra regels.
• Is er een "grondslag/rechtsgrond" om de persoonsgegevens te verzamelen, te ontvangen en te gebruiken? Er moet voor iedere verwerking (ieder soort gebruik) een grondslag/rechtsgrond zijn.
• Voor welke doeleinden worden de persoonsgegevens verzameld, ontvangen en verwerkt? De doeleinden moeten duidelijk zijn.
• Is het noodzakelijk om de persoonsgegevens te verzamelen, te ontvangen en verder te verwerken voor de vastgestelde doeleinden? Als het niet noodzakelijk is voor die doeleinden of voor verenigbare doeleinden, dan zouden de gegevens niet moeten worden verzameld, ontvangen of verwerkt.
• Wordt er gebruik gemaakt van "uitsluitend geautomatiseerde individuele besluitvorming", waaronder profiling, die rechtsgevolgen heeft voor de betrokken personen of die de personen op een andere manier in aanzienlijke mate raakt? Dit mag alleen onder bepaalde voorwaarden.
Waar nodig voert It Fits Human Protection een privacy-toets uit om antwoord te geven op de bovenstaande vragen.

C.3. OVERZICHT VERWERKINGEN
It Fits Human Protection houdt intern een overzicht bij van de verschillende verwerkingen waarvoor It Fits Human Protection is aan te merken als verantwoordelijke. Als It Fits Human Protection is aan te merken als "bewerker" van bepaalde persoonsgegevens, wordt ook een overzicht bijgehouden van de verwerkingen waarvoor It Fits Human Protection is aan te merken als bewerker.

C.4. GEHEIMHOUDING
Medewerkers van It Fits Human Protection houden de persoonsgegevens geheim en gebruiken deze alleen in het kader van hun werkzaamheden voor It Fits Human Protection . Zij verbinden zich hier schriftelijk toe richting It Fits Human Protection.

C.5. DATAKWALITEIT
Persoonsgegevens worden zoveel mogelijk juist, volledig en up-to-date gehouden.

C.6. PRIVACY BY DESIGN EN BY DEFAULT
Bij het ontwikkelen van (nieuwe) producten of diensten, waaronder IT-systemen wordt zoveel mogelijk gebruik gemaakt van “privacy by design” en “privacy by default”.
Privacy by design houdt samengevat in dat waar mogelijk rekening wordt gehouden met de bescherming van persoonsgegevens, bijvoorbeeld door gegevens te pseudonimiseren, en dat er wordt gezorgd voor data-minimalisatie en voor naleving van de privacyregels.
Privacy by default houdt samengevat in dat er voor wordt gezorgd dat als uitgangspunt alleen noodzakelijke persoonsgegevens worden gebruikt, dit gezien de hoeveelheid persoonsgegevens, de manier waarop zij worden gebruikt, de termijn waarbinnen ze worden opgeslagen en de toegankelijkheid daarvan. De maatregelen moeten er voor zorgen dat de persoonsgegevens als uitgangspunt niet zonder dat een medewerker van It Fits Human Protection daaraan te pas komt aan een onbeperkt publiek beschikbaar wordt gemaakt, bijvoorbeeld op het internet.

C.7. PIA’s (PRIVACY IMPACT ASSESSMENTS) EN PRIVACY TOETSEN
Bij het gebruik van persoonsgegevens met een hoog risico, zoals in ieder geval grootschalig gebruik van bijzondere persoonsgegevens, van geautomatiseerde individuele besluitvorming, waaronder profiling, die rechtsgevolgen heeft voor de betrokken personen of die de personen op een andere manier in aanzienlijke mate raakt of van het systematisch monitoren van een publieke ruimte op grote schaal, wordt een privacy impact assessment (PIA) uitgevoerd.
Bij nieuwe projecten waarbij persoonsgegevens worden verwerkt, wordt een privacy-toets gedaan om na te gaan of aan de privacyregels wordt voldaan.
De FG wordt betrokken bij het uitvoeren van de PIA en de privacy-toets.

C.8. EXTERN GEBRUIK VAN PERSOONSGEGEVENS
Als uitgangspunt geldt dat It Fits Human Protection de persoonsgegevens alleen voor zichzelf gebruikt.
In bepaalde gevallen kan het echter noodzakelijk zijn persoonsgegevens aan externe partijen door te geven. Bij het doorgeven van de persoonsgegevens aan externe partijen moet worden afgewogen of dat kan en zo ja, onder welke voorwaarden:
• Is de externe partij aan te merken als een “bewerker” die uitsluitend handelt in opdracht van It Fits Human Protection bij het in ontvangst nemen en gebruiken van persoonsgegevens? Dan worden er in een bewerkersovereenkomst afspraken gemaakt met een dergelijke partij over hoe ze met de persoonsgegevens omgaan. Dergelijke partijen mogen de persoonsgegevens niet voor eigen doeleinden gebruiken.
• Is de externe partij zelf aan te merken als “verantwoordelijke” – bijvoorbeeld de verzekeraar van It Fits Human Protection ? Dan moet worden getoetst of het doorgeven van persoonsgegevens aan deze externe partij overeenstemt met de vastgestelde doeleinden, welke persoonsgegevens daar noodzakelijk voor zijn en of er een grondslag is voor het doorgeven van de gegevens. Waar mogelijk worden afspraken vastgelegd over de uitwisseling van de persoonsgegevens.
• Is de externe partij voor de betreffende verwerking van persoonsgegevens aan te merken als verantwoordelijke samen met It Fits Human Protection ? Dan worden de afspraken over de persoonsgegevens vastgelegd in een overeenkomst tussen It Fits Human Protection en de andere verantwoordelijke.
• Is de externe partij een overheidsinstantie? Als uitgangspunt geeft It Fits Human Protection alleen persoonsgegevens aan overheidsinstanties door wanneer zij daartoe wettelijk verplicht is. In bepaalde specifieke situaties kan It Fits Human Protection echter ook genoodzaakt zijn persoonsgegevens door te geven aan een overheidsinstantie als er geen wettelijke verplichting is. Een voorbeeld hiervan is het doorgeven van gegevens over een persoon aan de politie als It Fits Human Protection aangifte doet tegen deze persoon. Er worden niet meer gegevens doorgegeven dan noodzakelijk.

C.9. DOORGIFTE NAAR BUITEN DE EER
Als persoonsgegevens worden doorgeven naar een land buiten de Europese Economische Ruimte ("EER"), (de EER bestaat uit de landen van de Europese Unie, Noorwegen, IJsland en Liechtenstein), waar geen passend beschermingsniveau voor de privacy is, worden maatregelen getroffen om die doorgifte juridisch mogelijk te maken.

C.10. BEVEILIGING EN DATALEKKEN
Persoonsgegevens moeten technisch en organisatorisch worden beveiligd op een passende manier, rekening houdend met de aard van de gegevens, de risico’s van het gebruik van de persoonsgegevens, de kosten van beveiliging en de stand van de techniek. It Fits Human Protection hanteert hiervoor een beveiligingsbeleid.
Als zich datalekken voordoen waarbij persoonsgegevens zijn betrokken, worden deze, als dat nodig is, gemeld aan de Autoriteit Persoonsgegevens en de betrokken personen. Er kunnen bijzondere omstandigheden zijn waaronder melding niet plaatsvindt.

C.11. BEWAREN PERSOONSGEGEVENS
Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor ze zijn verzameld. Waar toepasselijk wordt een bewaarbeleid en/of bewaarprotocol opgesteld.

C.12. RECHTEN VAN DE PERSONEN
De personen om wiens persoonsgegevens het gaat kunnen met betrekking tot hun persoonsgegevens bepaalde rechten richting It Fits Human Protection uitoefenen.
Het gaat om de volgende rechten:
• Een overzicht in begrijpelijke vorm te ontvangen van de persoonsgegevens.
• Informatie te ontvangen over het gebruik van de persoonsgegevens door It Fits Human Protection .
• Een kopie te ontvangen van de persoonsgegevens.
• In bepaalde gevallen de gegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en op verzoek aan een andere “verantwoordelijke” te laten doorzenden.
• Correctie van onjuiste gegevens en aanvulling van onvolledige gegevens.
• In bepaalde gevallen om verwijdering te vragen van hun persoonsgegevens.
• In bepaalde gevallen om “beperking” te vragen van hun persoonsgegevens.
• In bepaalde gevallen om bezwaar te maken tegen het verwerken van hun persoonsgegevens.
• Bij gebruik van persoonsgegevens voor direct marketing doeleinden geldt dat de persoon zich altijd mag verzetten en dat gebruik wordt gestaakt.
• Als uitgangspunt om een eenmaal gegeven toestemming weer in te trekken.
• Om een klacht in te dienen bij de Autoriteit Persoonsgegevens.
In bepaalde gevallen mag It Fits Human Protection een verzoek afwijzen, bijvoorbeeld als de persoon verzoekt om verwijdering van bepaalde persoonsgegevens maar deze nog moeten worden bewaard ten behoeve van een wettelijke verplichting. It Fits Human Protection laat de persoon dit dan weten. Waar van toepassing wordt een protocol gemaakt voor het omgaan met verzoeken van de personen.

C.13. INFORMEREN PERSONEN
De personen worden waar nodig geïnformeerd omtrent het gebruik van hun persoonsgegevens, bijvoorbeeld door middel van privacyverklaringen.

C.14. PROTOCOLLEN / RICHTLIJNEN / GEDRAGSCODES
Bij gebruik van persoonsgegevens met een ingrijpend karakter of een andere activiteit die aanzienlijk op de privacy van de personen ingrijpt, wordt als uitgangspunt een protocol, richtlijn en/of gedragscode opgesteld waarin wordt vastgelegd hoe met de gegevens en privacy om wordt gegaan.

C.15. TRAINING EN "AWARENESS"
It Fits Human Protection probeert zo veel mogelijk "awareness" te creëren over hoe met de persoonsgegevens om moet worden gegaan. Waar toepasselijk worden trainingen gegeven om de medewerkers te informeren.

C.16. FUNCTIONARIS GEGEVENSBESCHERMING ("FG")
It Fits Human Protection heeft een "Functionaris Gegevensbescherming" ("FG"). De FG dient (minimaal) als vraagbaak voor vragen over het gebruik van persoonsgegevens (zowel voor medewerkers van It Fits Human Protection als de betrokkenen), verstrekt advies over uit te voeren PIA´s en ziet toe op de naleving daarvan, ondersteunt bij projecten waarbij persoonsgegevens worden gebruikt en houdt intern toezicht op het gebruik van de persoonsgegevens door It Fits Human Protection . De FG is Mara van der Ven, directielid.

D. WIJZIGINGEN VAN DIT PRIVACYBELEID
Dit privacy-beleid kan worden aangepast, bijvoorbeeld om (beter) aan te sluiten op nieuwe wet- en regelgeving of gewijzigde omstandigheden. De FG wordt actief bij wijzigingen betrokken. De stakeholders worden over belangrijke wijzigingen geïnformeerd.

E. KLACHTEN
Wanneer een persoon om wiens persoonsgegevens het gaat een klacht heeft over het gebruik van zijn of haar persoonsgegevens, kan de persoon daar een klacht over indienen bij It Fits Human Protection . Hiervoor wordt een contactpunt aangewezen, waar toepasselijk per categorie personen of persoonsgegevens. De FG wordt op de hoogte gebracht van de klacht.
Als het de klager en het contactpunt (met hulp van de FG) niet lukt om de klacht onderling af te handelen, kan de persoon de klacht escaleren naar de manager van het contactpunt of naar de FG. Als het de manager of de FG niet lukt om een klacht met de klager af te handelen, dan kan de klacht worden geëscaleerd naar het management.
Als het management de klacht niet af kan handelen, dan zou de persoon kunnen besluiten om de rechter te vragen een beslissing te nemen of de Autoriteit Persoonsgegevens te vragen om bemiddeling. Alle klachten worden geregistreerd in het daarvoor gebruikte systeem.
Specifieke klachtenreglementen, zoals voor werknemers of consumenten, gaan vóór deze klachtenregeling.

BIJLAGE 1 – BEGRIPPEN
Persoonsgegevens: dit zijn gegevens (informatie) met betrekking tot een geïdentificeerde of identificeerbare persoon.

Uitsluitend geautomatiseerde individuele besluitvorming: dit is besluitvorming over de betrokkene die uitsluitend geautomatiseerd tot stand komt, dus zonder dat een mens bij die besluitvorming is betrokken.
Bijzondere persoonsgegevens: zijn de volgende soorten persoonsgegevens:
a. over de gezondheid,
b. over iemands ras of etnische achtergrond,
c. over iemands geloof of levensovertuiging,
d. over iemands seksuele gedrag of gerichtheid,
e. over iemands politieke opinies,
f. over iemands lidmaatschap van een vakbond,
g. genetische kenmerken,
h. biometrische kenmerken bedoeld om iemand te identificeren.
Ook het BSN en strafrechtelijke gegevens gelden als bijzonder persoonsgegeven die alleen mogen worden gebruikt als daar een in de AVG genoemde uitzondering voor geldt.
Verantwoordelijke: de “verantwoordelijke” is de partij die bepaalt wat er met de persoonsgegevens gebeurt en hoe dat gebeurt (deze bepaalt het “doel en de middelen”).
Betrokkene: een “betrokkene” is een persoon op wie de persoonsgegevens betrekking hebben.
Verwerking: een “verwerking” is een handeling met de persoonsgegevens. Daaronder valt o.a.: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden, combineren, afschermen wissen of vernietigen.
Grondslag/rechtsgrond: voor iedere verwerking met persoonsgegevens is één van de volgende grondslagen (ook wel "rechtsgronden") nodig:
a. geïnformeerde, vrije en specifieke toestemming,
b. omdat het noodzakelijk is voor het voorbereiden of uitvoeren van een overeenkomst met of ten behoeve van de betrokkene,
c. omdat het noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verantwoordelijk rust,
d. omdat het noodzakelijk is om de vitale belangen van de betrokkene (of een andere persoon) te beschermen,
e. omdat het noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verantwoordelijke is opgedragen, of
f. omdat het noodzakelijk is voor een gerechtvaardigd belang van de verantwoordelijke of een derde dat vóór het belang van de betrokkene gaat.