Johan

JOHAN Portaal - Eigenaarschap van data, borging privacy en de AVG

Versie: 1.5.1
Laatste revisie: 30-03-2020
Status: Goedgekeurd
Opsteller: Gertjan Westerlaken

Samenvatting

Dit document beschrijft de aanpak van JOHAN om aan contractuele en wettelijke eisen vanuit de AVG te voldoen. Het beschrijft:

- Rol en positie van de diverse actoren in het ecosysteem van het JOHAN Portaal
- De diverse categorieën van data in het JOHAN Portaal en het bijbehorende eigenaarschap
- De dataflow van een typisch project in het JOHAN Portaal
- De persoonsgegevens die verwerkt worden in het JOHAN Portaal
- Wie in JOHAN als verwerker en wie als verwerkingsverantwoordelijke kan worden aangemerkt
- Grondslagen voor verwerking, doelbinding en bewaartermijnen
- Het JOHAN ecosysteem
- De uitgangspunten voor JOHAN's privacybeleid m.b.t. privacy-by-design en privacy-by-default
- De toepassing van privacy-by-design en privacy-by-default principes
- De privacy beschermende maatregelen die JOHAN neemt
- De contractuele eisen waar JOHAN aan moet voldoen en de aanpak om daar aan te voldoen
- De eisen uit de AVG uitvoeringswet en de aanpak van JOHAN om daaraan te voldoen

Audience

Dit document is openbaar. Het is bedoeld voor iedereen die zich wil informeren over de manier waarop JOHAN complicance met AVG waarborgt, waaronder bijv. de FG, security- en privacy officers, IT managers, inkopers, procurement managers, business case managers en projectmanagers.

Link met andere relevante documenten

Privacy gerelateerde documenten van JOHAN, classificatie “openbaar”:

- Privacybeleid Johan BV
- DPIA JOHAN Portaal
- Privacyverklaring JOHAN BV t.b.v. de eindgebruikers
- Verklaring geografische beperking dataopslag

Security gerelateerde documenten van JOHAN, classificatie “openbaar”:

- Beleid Informatiebeveiliging Johan BV
- ISO 27001 Verklaring van toepasselijkheid
- ISO 27001 Certificaat

Intern vertrouwelijke documenten, op verzoek ter inzage:

- Hoofdlijnendocument Johan BV
- Technische beschrijving en security aspecten Johan Portaal
- Beveiligingsnormen voor systeemontwikkeling
- Risico assessment en behandel methodiek Johan BV
- Continuïteitsplan Johan BV

Inhoud

1. Inleiding

JOHAN werkt met werknemers, werkgevers, dienstverleners en wetenschappelijke instituten samen aan duurzame inzetbaarheid. JOHAN levert een online SAAS oplossing (het JOHAN Portaal) waarmee bedrijven die aandacht willen besteden aan duurzame inzetbaarheid een scala aan (on- en offline) meetinstrumenten wordt geboden die het bedrijf in staat stellen de gezondheid en vitaliteit van hun medewerkers (voor de individuele medewerker) in kaart te brengen en deze middels diverse interventie programma's te verbeteren.

JOHAN heeft privacy van haar gebruikers hoog in het vaandel. In het JOHAN Portaal wordt data opgeslagen door diverse partijen: werkgevers, contentleveranciers, professionals en eindgebruikers (werknemers, burgers). Eigenaarschap is de basis om data af te schermen tussen de diverse partijen. Door het consequent toepassen van privacy-by-design en privacy-by-default principes wordt privacy gegarandeerd.

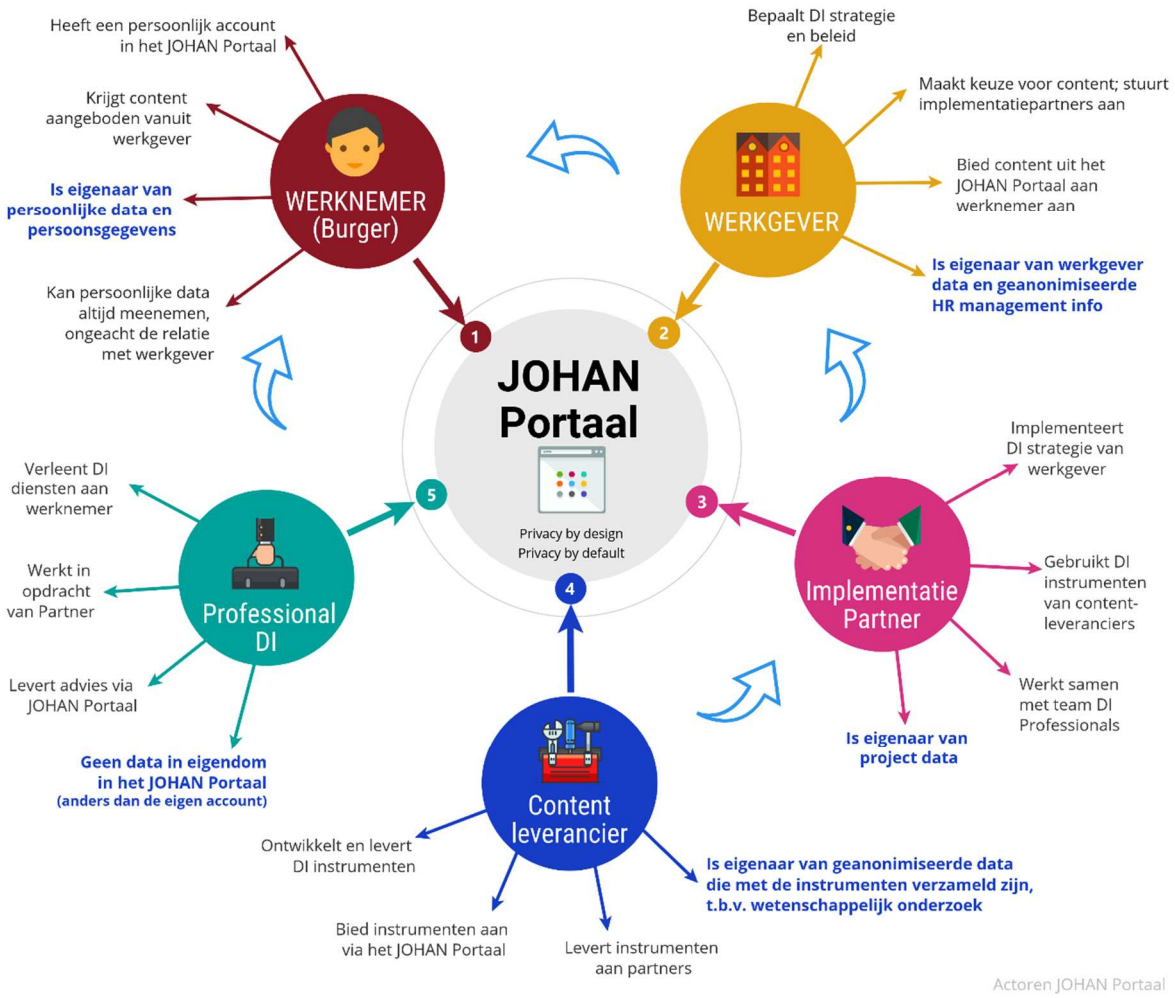
Doordat JOHAN persoonsgegevens verwerkt, deze gegevensverwerking plaatsvindt binnen de EU en het geen uitzondering betreft op het materiële toepassingsbereik van de AVG, is automatisch de AVG van toepassing. JOHAN heeft hierbij – afhankelijk om welke data het gaat – zowel de rol van verwerker als die van verwerkingsverantwoordelijke.

Dit document beschrijft de volgende aspecten:

- Rol en positie van de diverse actoren in het ecosysteem van het JOHAN Portaal
- De diverse categorieën van data in het JOHAN Portaal en het bijbehorende eigenaarschap
- De dataflow van een typisch project in het JOHAN Portaal
- De persoonsgegevens die verwerkt worden in het JOHAN Portaal
- Wie in JOHAN als verwerker en wie als verwerkingsverantwoordelijke kan worden aangemerkt
- Grondslagen voor verwerking, doelbinding en bewaartermijnen
- Het JOHAN ecosysteem
- De uitgangspunten voor JOHAN's privacybeleid m.b.t. privacy-by-design en privacy-by-default
- De toepassing van privacy-by-design en privacy-by-default principes
- De privacy beschermende maatregelen die JOHAN neemt
- De contractuele eisen waar JOHAN aan moet voldoen en de aanpak om daar aan te voldoen
- De eisen uit de AVG uitvoeringswet en de aanpak van JOHAN om daaraan te voldoen

2. Actoren, eigenaarschap en data in het JOHAN Portaal

Het JOHAN Portaal is een digitaal platform ter ondersteuning van het werken aan duurzame inzetbaarheid (DI) en aanverwante thema's. Het is een legodoos met functionaliteiten, instrumenten en content op het gebied van duurzame inzetbaarheid. Het JOHAN Portaal is te zien als een DI **ecosysteem** waar de volgende actoren in samenkomen:

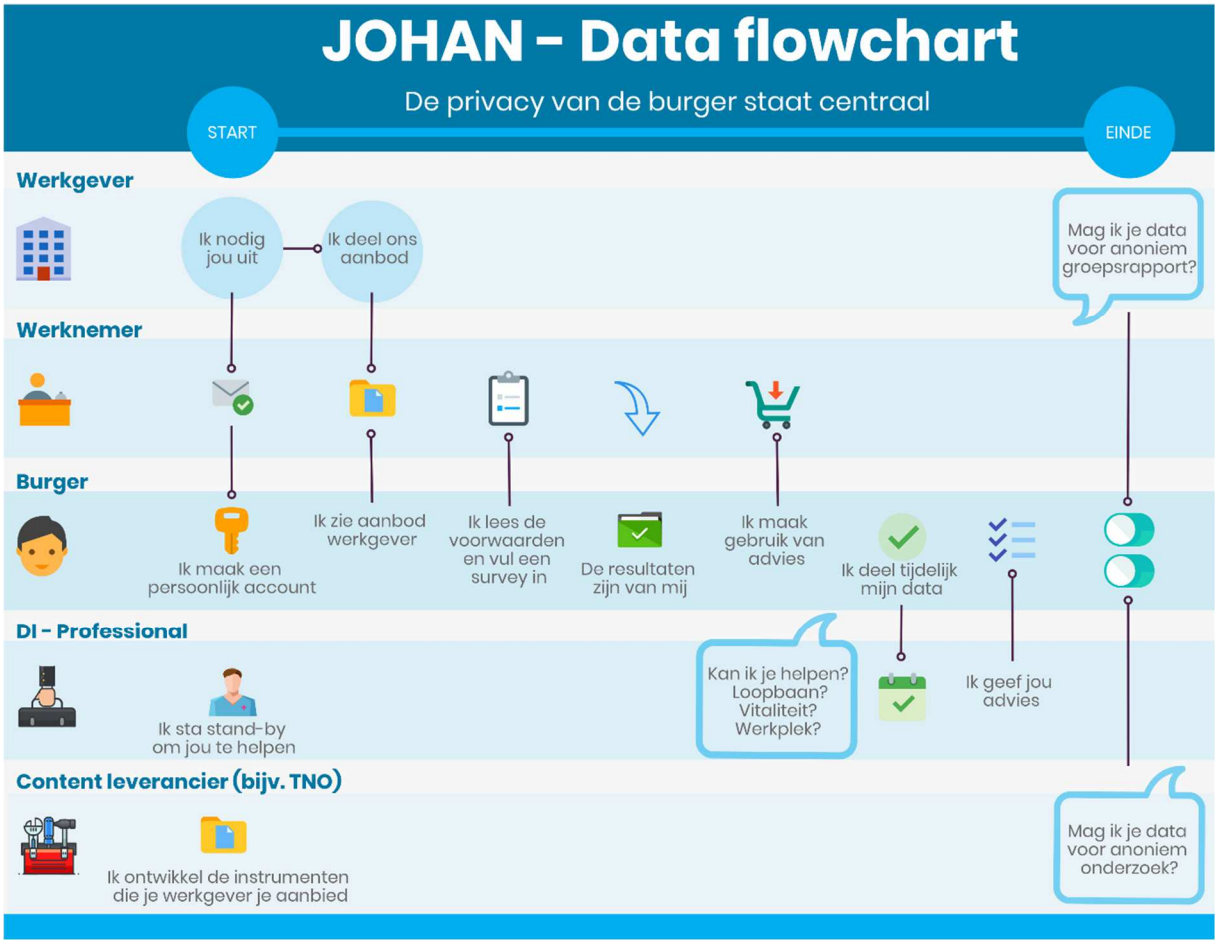


Actoren JOHAN Portaal

- **Werkenden** worden met behulp van een persoonlijke leercyclus met daarin slimme instrumenten, een marktplaats met interventies, actieplannen en leerervaringen ondersteund om te werken aan hun eigen gezondheid en inzetbaarheid.
- **Aanbieders (werkgevers, opleiders en branche-organisaties)** worden met behulp van procestools en managementinformatie ondersteund bij het ontwikkelen en uitvoeren van een passende implementatiestrategie.
- **Dienstverleners en implementatiepartners** worden ondersteund met behulp van een kwaliteitssysteem voor het ontwikkelen en verbeteren van interventies.
- **Contentleveranciers, zoals kennisinstituten en andere publieke instanties** worden gefaciliteerd met informatie/data om de markt kennis terug te geven die nodig is om implementatiestrategie, interventies en nieuwe innovaties door te ontwikkelen.
- **DI-Professionals**, - zoals coaches, loopbaanspecialisten, Arbo specialisten, (para)medici en psychologen -, kunnen vanuit één omgeving communiceren en advies geven aan werkenden.

2.1. Dataflow in het JOHAN Portaal

De standaard dataflow in het JOHAN Portaal is zichtbaar in onderstaande flowchart. In deze weergave staat de rol van de burger centraal, om daarmee het onderscheid te maken met de *werknemer*. Hoewel de werknemer voor de werkgever centraal staat, is de data die de werknemer gedurende een traject toevoegt aan zijn/haar profiel, geen eigendom van die werkgever, maar van het individu.



Toelichting flowchart.

De werkgever maakt aan de hand van het eigen DI beleid een keuze uit het aanbod van content leveranciers. De implementatie partner adviseert hierbij en richt het JOHAN Portaal in. Hierna wordt de werknemer uitgenodigd door de werkgever om gebruik te maken van diens aanbod. Deze uitnodiging kan per e-mail op het zakelijke e-mail adres, of via een “open inschrijvingslink”. Beide methoden geeft de werknemer de mogelijkheid een JOHAN account aan te maken c.q. het aanbod van de werkgever toe te voegen aan zijn of haar bestaande account. Na het aanmaken van de account c.q. het accepteren van het aanbod, maakt de werknemer gebruik van de aangeboden content. Indien de aangeboden content persoonlijke data vergaart, wordt deze eigendom van de burger en komt in zijn of haar “**burgerkluis**”. De burgerkluis in het JOHAN Portaal bevat alle persoonsgegevens en persoonlijke data die een betrokkene toevoegt aan zijn of haar profiel, door het gebruik van diensten en/of producten in het JOHAN Portaal. Het gaat dan bijvoorbeeld om resultaten van surveys, data uit self-assessments en afgenomen content. Andere actoren hebben

standaard geen toegang tot deze data. Duurzame Inzetbaarheid Professionals, zoals coaches, loopbaanbegeleiders, arbospecialisten, psychlogen of (para)medici kunnen data toevoegen aan de burgerkluis. Denk hierbij aan adviezen of diagnostische (medische) gegevens uit bijvoorbeeld een PMO. (Preventief Medisch Onderzoek.) Deze data wordt daarmee direct expliciet eigendom van de burger; nadat het is toegevoegd door een DI professional heeft die daar geen toegang meer toe of zeggenschap over. Ook kan een burger expliciet advies vragen aan een DI professional. De burger kan hierbij de DI professional tijdelijk toegang geven tot (delen van) zijn of haar persoonlijke data.

Als laatste kan de burger in de privacy settings van het JOHAN Portaal aangeven of hij/zij akkoord gaat met het delen van geanonimiseerde data ten behoeve van HR groepsrapportages (eigendom werkgever) en het delen van geanonimiseerde data ten behoeve van wetenschappelijk onderzoek (eigendom contentleverancier)[1].

2.2. Eigenaarschap van data

Ieder type data hoort bij één eigenaar en niet meer dan bij één eigenaar. De eigenaar bepaalt wat er met deze data gebeurt, bepaalt veelal de bewaartermijn en is als enige in staat deze data te muteren of te verwijderen. Om welke data dit gaat is, is in de volgende paragrafen beschreven.

Het eigenaarschap is mede bepalend in de rol die de betreffende actor heeft met betrekking tot de verwerking van de persoonsgegevens. (i.c.: wie als verwerkingsverantwoordelijke en wie als verwerker wordt aangemerkt.)

[1] NB: De genoemde privacy dashboard settings in deze alinea zijn in ontwikkeling, planning Q3-2020. Voor die tijd dient goedkeuring voor het gebruik van geanonimiseerde data ten behoeve van HR groepsrapportages (eigendom werkgever) en het delen van geanonimiseerde data ten behoeve van wetenschappelijk onderzoek geregeld te worden via gebruikersvoorwaarden van de aanbieder en contentleverancier.

3. Persoonsgegevens in het JOHAN Portaal

3.1. Inleiding

In het JOHAN Portaal wordt data van verschillende actoren opgeslagen. Allereerst uiteraard de individuele burger, die doorgaans het account aangeboden krijgt vanuit de werkgever of andere aanbieder. De burger accounts vormen de grootste gebruikersgroep. Daarnaast zijn er andere types accounthouders: de aanbieder (werkgever); de implementatiepartner; de contentleverancier; de DI-professional.

Voor elk van deze actoren c.q. typen accounthouders zijn verschillende persoonsgegevens, grondslagen, doelbindingen en bewaartermijnen van toepassing.

In dit hoofdstuk wordt per actor uiteengezet:

- Welke persoonsgegevens in het JOHAN Portaal zijn opgeslagen;
- Voor welke doelen de persoonsgegevens worden verwerkt;
- Wat de grondslagen zijn voor de verwerking;
- Hoe de data wordt verzameld;
- Welke actoren verwerkingsverantwoordelijke zijn en welke verwerker;
- Welke overeenkomst(en) en gebruikersvoorwaarden er van toepassing zijn op de verwerking;
- Welke bewaartermijnen van toepassing zijn.

3.2. Welke actoren zijn verwerkingsverantwoordelijk en welke verwerker?

In De volgende paragrafen is weergegeven welke persoonsgegevens in het JOHAN Portaal worden opgeslagen. De paragrafen met tabellen zijn ingedeeld aan de hand van het eigenaarschap en de bijbehorende actor, i.c.: per type accounthouder.

Hoewel de AVG weinig zegt over eigenaarschap van data, is dit in het JOHAN op een logische manier gebonden aan de aard van de verwerking en – mede daar uit afgeleid – wie aangemerkt kan worden als verwerkingsverantwoordelijke en als verwerker. In onderstaande is e.e.a. verder uitgewerkt. Ook de bewaartermijnen zijn direct gerelateerd aan de aard van de verwerking en het eigenaarschap.

3.3. Persoonsgegevens, grondslagen, doelbinding en bewaartermijnen per actor

In de volgende paragrafen wordt per type accounthouder een overzicht gegeven van hetgeen in de inleiding is opgesomd. Voor alle accounthouder geldt dat zij de rechten die hun vanuit de AVG zijn toegekend, kunnen uitoefenen via self-serive en/of via de supportdesk van JOHAN.

3.3.1. LICENTIE VOOR WERKGEVER, DI PROFESSIONAL EN CONTENTLEVERANCIER

Invoer: Data wordt ingevoerd door accounthouder.

Wettelijke grondslag: noodzakelijk voor de uitvoering van een overeenkomst.

Voorwaarden voor gebruik zijn beschreven in de licentieovereenkomst en SLA (service level agreement) tussen JOHAN en Licentienemer. Persoonsgegevens zijn benoemd in de verwerkersovereenkomst tussen JOHAN en licentienemer.

Persoonsgegevens	Doel	Bewaartermijn	Verwerking
▪ **Persoonsnaam** ▪ **Zakelijk emailadres** ▪ **Mobiele telefoonnummer**	▪ Toegang tot het JOHAN Portaal door Licentienemer ▪ Leveren van support door JOHAN aan Licentienemer ▪ 2FA ▪ Contactinformatie	Wordt bepaalt door de contractduur tussen de onderlinge partijen.	Licentienemer is verwerkings-verantwoordelijke, JOHAN verwerker.

3.3.2. LICENTIE VOOR INDIVIDUELE BURGER

Invoer: Data wordt ingevoerd door accounthouder.

Wettelijke grondslag: expliciete toestemming van de betrokkene.

Voorwaarden voor gebruik zijn beschreven in overeenkomst tussen JOHAN en Licentienemer (burger) en in het privacystatement van JOHAN, zoals aangeboden worden bij het aanmaken van een JOHAN account. De accounthouder is de eigenaar van de persoonsgegevens.

Persoonsgegevens	Doel	Bewaartermijn	Verwerking
▪ **Persoonsnaam** ▪ **Privé emailadres** ▪ **Mobiele telefoonnummer** ▪ **Geboortedatum**	▪ Toegang tot het JOHAN Portaal door Licentienemer ▪ Leveren van support door JOHAN aan Licentienemer ▪ 2FA ▪ Contactinformatie	Zolang als licentienemer zijn/haar account actief houdt.	JOHAN is verwerkings-verantwoordelijke

3.3.3. WERKNEMER DATA

Invoer: Invoer en eigenaarschap ligt bij de verwerkingsverantwoordelijke, i.c. de *aanbieder* van het account en de content. Gewoonlijk is dit de werkgever, branche-organisatie of opleidingsinstituut.

Wettelijke grondslag: noodzakelijk voor de uitvoering van een overeenkomst.

Voorwaarden voor gebruik zijn beschreven in de licentieovereenkomst tussen aanbieder en de partij die de licentie verstrekt aan de aanbieder, i.c.: de implementatiepartner of JOHAN. Persoonsgegevens zijn benoemd in de verwerkersovereenkomst tussen aanbieder en licentieverstrekker.

De licenties kunnen door twee partijen aan de aanbieder worden verstrekt:

1. **De aanbieder neemt licenties af bij de DI dienstverlener**. In dit geval zijn er twee verwerkersovereenkomsten van toepassing:
    a. tussen aanbieder en DI dienstverlener. De aanbieder is verwerkingsverantwoordelijke, de DI dienstverlener verwerker.
    b. Aangezien de DI dienstverlener de werknemersdata gaat onderbrengen in het JOHAN Portaal, is er ook een verwerkersovereenkomst tussen de DI dienstverlener en JOHAN. De DI dienstverlener is hierbij verwerkingsverantwoordelijke, JOHAN verwerker. (Ten opzichte van de aanbieder kan JOHAN worden gezien als subverwerker.)

2. **De aanbieder neemt licenties rechtstreeks bij JOHAN af**. In dit geval is er één verwerkersovereenkomst van toepassing, namelijk tussen aanbieder (verwerkingsverantwoordelijke) en JOHAN (verwerker).

Persoonsgegevens	Doel	Bewaartermijn	Verwerking
▪ **Zakelijke emailadres** ▪ **Afdeling** ▪ **Functie** ▪ **Personeelsnummer** ▪ **Andere kenmerken**	▪ Aanbieden van content op het JOHAN Portaal aan werknemers, evt. gesegmenteerd voor specifieke doelgroepen ▪ Categoriseren werknemers voor geanonimiseerde, niet-herleidbare management-informatie	Wordt bepaalt door de contractduur tussen JOHAN en werkgever.	Aanbieder is verwerkings-verantwoordelijke, licentieverstrekker is verwerker.

Op het zakelijk e-mail adres wordt de werknemer uitgenodigd om gebruik te maken van het werkgevers aanbod op het JOHAN Portaal. Met behulp van een link kan de werknemer een nieuw JOHAN account aanmaken op zijn/haar eigen e-mail adres, c.q. het werkgeversaanbod toevoegen aan zijn/haar JOHAN account. Voorwaarden voor het gebruik liggen bij de aanbieder en contentleverancier.

3.3.4. BURGER DATA

Invoer: Door de betrokkene zelf (accounthouder / burger) en door DI professionals.

Wettelijke grondslag: expliciete toestemming van de betrokkene. (Gegeven bij het aanmaken van de JOHAN account)

Bewaartermijn: Zolang de accounthouder zijn/haar persoonlijk account actief houdt. Accounthouder kan het account ieder moment opheffen[2]. Het account en de bijbehorende onderstaande data ("burgerkluis") wordt daarbij definitief en onomkeerbaar verwijderd.

De burgerkluis bevat het volgende:

Persoonsgegevens	**Soort verwerking**	**Doel(einden) van de verwerking**	**Verwerking**
o Participatie producten (instrumenten, modules, etc.) o Status product o Verzonden emails	Betrokkene activeert zelfstandig deelname aan producten van Licentienemer na het verkrijgen van een persoonlijke registratielink hiervoor	o Uitvoeren proces voor bereiken optimale resultaten voor Betrokkene o Uitvoeren van betalingen / facturatie van gekochte producten o Verbetering van producten door Licentienemer	JOHAN is verwerkings-verantwoordelijke
o Scores op vragenlijsten / onderzoeken (zelf-assessment)	Betrokkene vult zelf de door Licentienemer toegewezen vragenlijst in en verkrijgt persoonlijke scores	o Inzicht in eigen situatie (irt referentiegroep) o Personaliseren aanbod producten obv het persoonlijke scoreprofiel o Verkrijgen niet-herleidbare managementinformatie voor inzicht in groepsresultaten	JOHAN is verwerkings-verantwoordelijke
o Scores op fysieke metingen o Adviezen van professionals	Professionals (bijv. coach, bedrijfsarts, arbo-deskundige of loopbaanadviseur) voert gegevens in voor betrokkene na uitvoering van een meting of gesprek	o Inzicht in eigen situatie (irt referentiegroep) o Advies met aanbevelingen voor betrokkene om verder te werken aan de eigen situatie	JOHAN is verwerkings-verantwoordelijke

[2] NB: De accounthouder dient periodiek in te loggen op het JOHAN Portaal om het account actief te houden. Na een periode van inactiviteit wordt een aantal reminders verzonden met de vraag of de betrokkene het account wil behouden. Het niet reageren op deze reminders leidt er uiteindelijk toe dat het account definitief wordt verwijderd.

3.3.5. DATA T.B.V. LOGGING EN BEVEILIGING

Bij alle accounthouders wordt er door de servers van JOHAN de volgende persoonsgegevens gelogd: datum- en tijd en status van aanmeldpogingen en webrequests op het JOHAN Portaal, incl. IP adres van de accounthouder. JOHAN is verwerkingsverantwoordelijke voor deze data. De wettelijke grondslag is toestemming van de betrokkene. Het doel van de verwerking is de beveiliging van de webapplicatie en het veilig houden van het gebruikersaccount. Deze data wordt niet gedeeld en wordt niet langer bewaard dan noodzakelijk.

Deze gegevens worden, afhankelijk om welke overeenkomst het gaat, vermeld in de licentie-overeenkomst en verwerkersovereenkomst of in het privacystatement als onderdeel van de gebruikersvoorwaarden.

3.4. Waarom is JOHAN verwerkingsverantwoordelijke voor de burgerkluis?

JOHAN is verwerkingsverantwoordelijke voor de data in de burgerkluis. Omwille van de volgende redenen is voor deze opzet gekozen:

- De burgerkluis staat los van degene die het persoonlijk account aan de werknemer aanbied. De aanbieder (werkgever, branche-organisatie of opleidingsinstituut) levert deze data niet aan JOHAN aan. De data wordt door de betrokkene zelf vergaart, of toegevoegd door DI professionals zoals arbeidscoaches, loopbaanbegeleiders etc.
- Omdat binnen het kader van de AVG de aanbieder (werkgever) in beginsel geen medische informatie mag verwerken van zijn werknemers, is het eigenaarschap van deze data bij de burger gelegd, niet bij de werknemer (en al zeker niet bij de werkgever).
- Het is niet mogelijk dat deze data terug geleverd kan worden aan de aanbieder, omdat de aanbieder deze data in beginsel nooit heeft aangeleverd ter verwerking.
- Omdat de aanbieder deze data in beginsel niet mag verwerken binnen het kader van de AVG en ook niet terug geleverd krijgt, kan deze data per definitie geen onderdeel zijn van een verwerkersovereenkomst waarin de aanbieder een partij is.
- Aangezien de burger de data die hij/zij vergaard heeft in de burgerkluis kan meenemen en behouden, staat die data los van de werkgever. De werknemer kan zijn dienstverband met de werkgever beëindigen, maar de data in de burgerkluis behouden. Zolang als de burger er voor kiest om zijn of haar account bij JOHAN aan te houden, is de burgerkluis voor hem of haar beschikbaar.
- Aangezien JOHAN verantwoordelijk is voor het beschikbaar houden van de persoonlijke account van de burger (zolang als die burger dat wenst), is het - gezien bovenstaande argumenten – het meest logisch als JOHAN verwerkingsverantwoordelijke is voor het persoonlijk account en de daarbij horende burgerkluis.
- Het doel dat JOHAN vastgesteld heeft voor deze verwerking is: “het beschikbaar kunnen stellen en houden van een persoonlijk account op het JOHAN Portaal, waarmee betrokkene toegang krijgt tot DI content van verschillende aanbieders”. Het middel is het JOHAN Portaal.

NB: De grondslag voor de verwerking is “expliciete toestemming van de betrokkene”. De hier uit voortvloeiende rechten kan de betrokkene zelf of via JOHAN laten uitoefenen. (Denk bijv. aan inzien van de persoonsgegevens, (laten) rectificeren, verwijderen of meenemen.)

3.5. Kunnen er andere persoonsgegevens worden verwerkt in het JOHAN Portaal?

Het is in beginsel mogelijk om aanvullende persoonsgegevens in het JOHAN Portaal te verwerken.

Indien de aanbieder en/of contentleverancier er voor kiest om aanvullende persoonsgegevens te verwerken in het JOHAN Portaal, bijvoorbeeld het vergaren van persoonsgegevens via vragenlijsten of instrumenten, dan zijn die partijen er verantwoordelijk voor dit op een manier te doen die in lijn is met huidige wet- en regelgeving. (Zaken als grondslag, doelbinding, transparantie, bewaartermijnen etc., bekrachtigd in aanvullende verwerkersovereenkomsten tussen die partijen en via gebruikersvoorwaarden c.q. privacystatements gecommuniceerd aan de betrokkene.)

Opgemerkt wordt dat dit buiten JOHAN omgaat en JOHAN (dus) geen verantwoordelijk draagt voor de verwerking van deze gegevens en uitsluitend als subverwerker in dit proces is aan te merken.

4. Ecosysteem JOHAN – positie van de diverse actoren

4.1. Overeenkomsten tussen de verschillende actoren

Zoals vermeld komen in het ecosysteem van JOHAN diverse actoren samen. De verantwoordelijkheden en rollen van iedere actor worden en de onderlinge positie worden verankerd in diverse overeenkomsten: licentie-overeenkomsten; verwerkersovereenkomsten, service level agreements en gebruikersvoorwaarden.

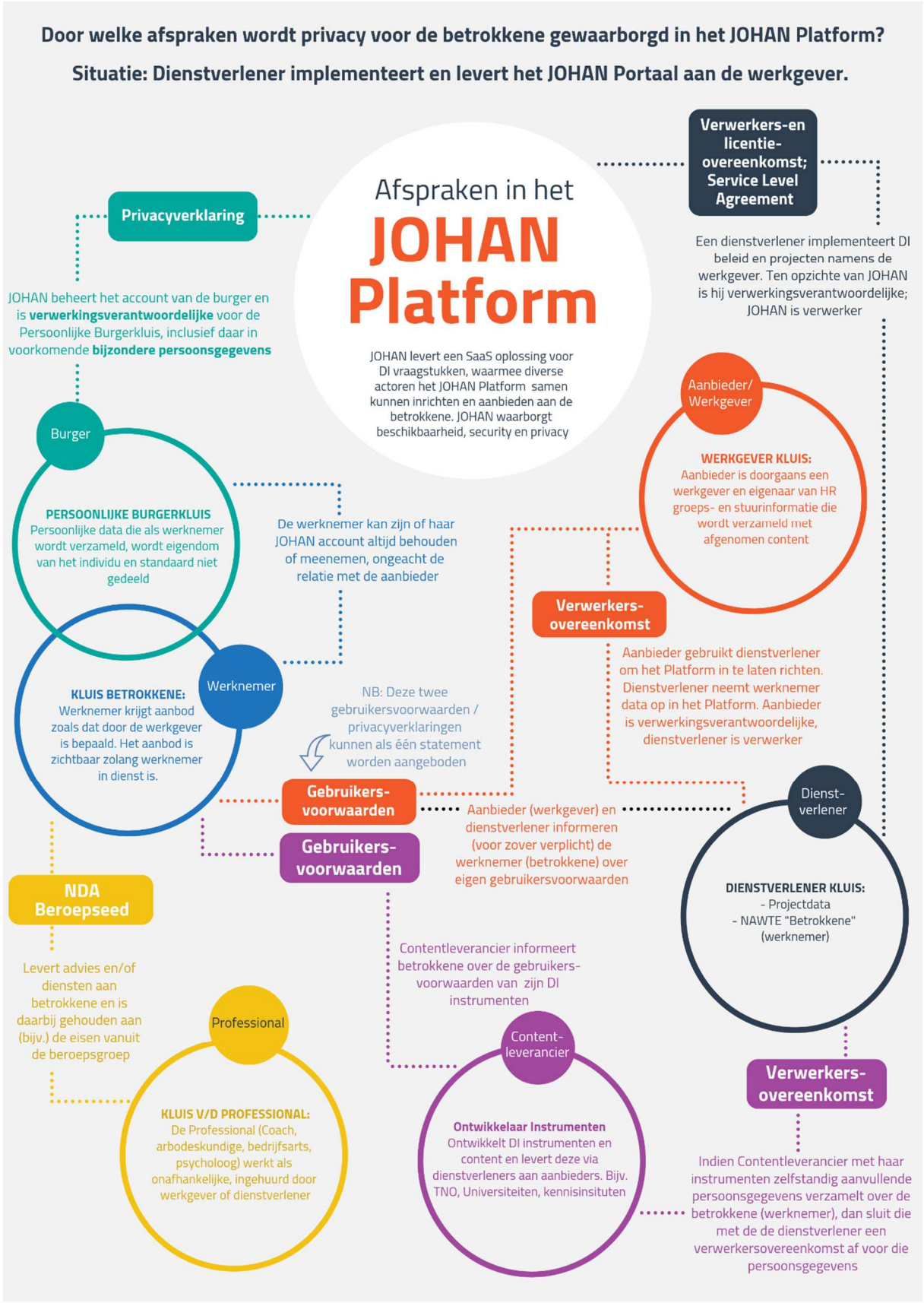
Er zijn twee manieren waarop licenties voor het JOHAN Portaal worden uitgeleverd:

1. JOHAN levert licenties voor het Portaal aan een DI dienstverlener. Deze dienstverlener treedt op als implementatiepartner en implementeert het JOHAN Portaal bij de aanbieder, i.c. de werkgever, branche-organisatie of opleidingsinstituut. De DI dienstverlener heeft het recht om gebruikerslicenties voor het Portaal aan de aanbieder te leveren (Standaard situatie)
2. JOHAN levert de licenties voor het gebruik rechtstreeks aan de aanbieder (werkgever, branche-organisatie of opleidingsinstituut). De werkgever implementeert zelf, eventueel met consultancy van derden of JOHAN.

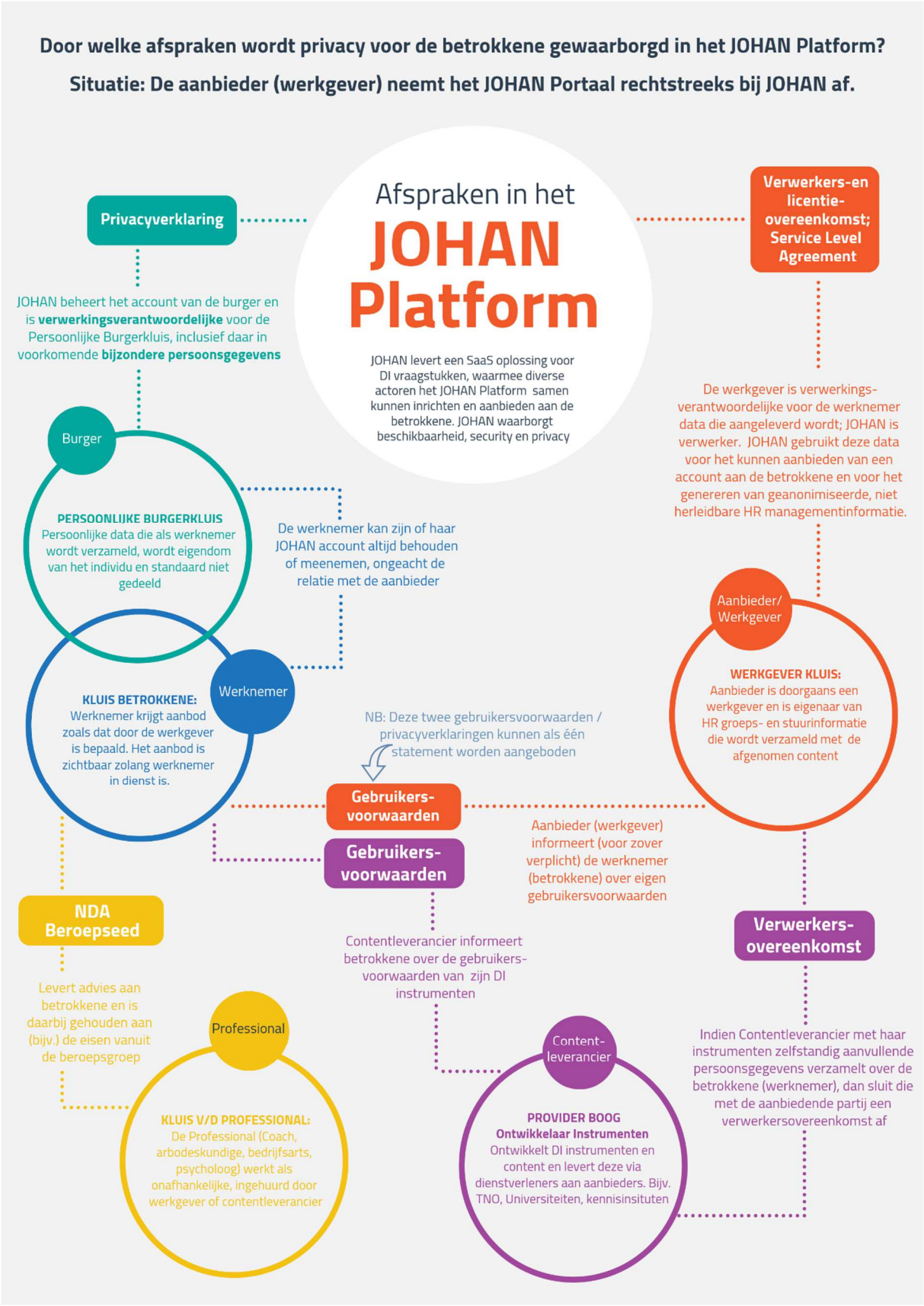
Beide situaties zijn schematisch weergegeven op de afbeeldingen op de volgende twee pagina's.

NB: Onderstaande schema's zijn niet bedoeld om een volledig beeld te geven van **alle** mogelijke overeenkomsten die tussen partijen gesloten worden of kunnen worden. De schema's zijn m.n. bedoeld om te laten zien welke overeenkomsten de actoren met JOHAN sluiten, en welke andere verwerkersovereenkomsten en gebruikersvoorwaarden er van toepassing (kunnen) zijn. Overige overeenkomsten tussen partijen, anders dan met JOHAN, zijn bewust en t.b.v. het behoud van overzicht niet opgenomen. (Bij overige overeenkomsten valt er te denken aan bijv. een reseller overeenkomst tussen contentleverancier en dienstverlener; een diensten overeenkomst tussen dienstverlener en aanbieder, etc. etc. Deze vallen uiteraard buiten de verantwoordelijkheid van JOHAN.)

1. Standaard situatie. Levering Portaal en implementatie via DI dienstverlener



2. Levering Portaal rechtstreeks aan de aanbieder



5. Maatregelen ter bescherming van de persoonsgegevens

5.1. Privacy beschermende maatregelen

De maatregelen die JOHAN neemt om de privacy komen voort uit ons privacybeleid en de periodiek uitgevoerde risicoanalyses en het bijbehorende risicobehandelingsplan.

De maatregelen zijn beschreven in met name hoofdstuk 5.3 als ook in hoofdstuk 6 en 7.
Deze hoofdstukken behandelen respectievelijk:

- Maatregelen die voortvloeien uit de toepassing van “Privacy by design” & “Privacy by default” principes (hfdst. 5.3)
- Aanpak om aan contractuele eisen te voldoen (hfdst. 6)
- Aanpak om aan eisen vanuit de AVG te voldoen (hfdst. 7)

5.2. Informatiebeveiligingsmaatregelen

De beveiligingsmaatregelen die JOHAN neemt om haar informatiebeveiligingsbeleid te borgen, zijn opgesomd in JOHAN’s ISO 27001:2017 verklaring van toepasselijkheid.

Deze verklaring van toepasselijkheid vloeit voort uit de risicobeoordeling die JOHAN periodiek uitvoert en het bijbehorende risicobehandelingsplan.

Het document bevat de beheerdoelstellingen en maatregelen uit bijlage A van de ISO/IEC 27001:2017 norm, (zijnde ISO/IEC 27002), die zijn gekozen en geïmplementeerd.

Daarnaast bevat onze verklaring van toepasselijkheid, onder hfst. A.19, een aantal eigen geselecteerde maatregelen, specifiek op het gebied van privacy, gegevensbescherming en compliance aan de AVG.

5.3. Link naar relevante documenten

De meest recente versie van onze **ISO 27001:2017 Verklaring van Toepasselijkheid** is in te zien op:

https://support.johan.nl/wp-content/uploads/Verklaring-van-Toepasselijkheid-ISO27001-Johan-BV-versie-1.1.pdf

De meest recente versie van ons **ISO 27001:2017 certificaat** is in te zien op:

https://support.johan.nl/wp-content/uploads/DigiTrust-Certificaat-ISO-27001-Johan-BV.pdf

Verklaring **beperking geografische opslag**, afgegeven door het datacenter dat het JOHAN Portaal host:

https://support.johan.nl/wp-content/uploads/Verklaring-geografische-beperking-dataopslag-True.pdf

5.4. Toepassing Privacy by design & Privacy by default principes

5.4.1. Uitgangspunten

JOHAN past diverse "*Privacy by design"* en "*Privacy by default"* principes toe in haar privacy beleid. De volgende uitgangspunten zijn gebaseerd op de privacy principes van het CIP (*Centrum Informatiebeveiliging en privacybescherming*) en maken onderdeel uit van ons privacybeleid:

- Privacy by Design geldt vanaf de initiatie van het ontwerp en niet achteraf. Starten met Privacy by Design start al bij de beleidsvorming.
- Privacycriteria gelden per default. Daarbij is de regel: "*pas toe of leg uit*".
- Privacymaatregelen zijn integraal onderdeel van de informatieverwerking en zijn geen add-on. Dit geldt voor de technische systemen én de organisatorische processen.
- Het waarborgen van de privacy is een verantwoordelijkheid van alle betrokkenen partijen. Het is niet een add-on op de criteria voor één partij.
- Privacy by Design waarborgt het privacymanagement, inclusief de beveiliging, gedurende de gehele levenscyclus van de persoonsgegevens. Het is niet een eenmalige actie.
- Inzicht en transparantie over hoe persoonsgegeven worden verwerkt moet mogelijk zijn voor zowel de betrokkene persoonlijk, als "eenieder, de eigen organisatie en toezichthouders".
- Technische en organisatorische maatregelen zijn pas effectief, wanneer zij de persoonlijke levenssfeer van de betrokkenen beschermen.

5.4.2. Gehanteerde strategieën en de daaruit voorvloeiende maatregelen

Hieronder volgt een overzicht van de belangrijkste privacy by design en privacy by default strategieën en de wijze waarop JOHAN die toepast:

Applicatie- en Ontwerp georiënteerde strategieën	
Gescheiden ontwikkel-, test-, acceptatie- en productie-omgevingen	▪ Persoonsgegevens komen uitsluitend voor in de productie-omgeving. Deze voldoet aan strenge normen. (Tier III datacenter dat aantoonbaar voldoet aan de ISO27001, NEN 7510 en ISO9001 norm.) ▪ Toegang tot de productie-omgeving is strikt gelimiteerd door toepassing van een autorisatie-matrix. ▪ Toepassing van vier-ogen principe bij wijzigingen in de productie-omgeving.
Sterke authenticatie	▪ Voor i*edere* account in het JOHAN Portaal is 2 factor authenticatie verplicht. ▪ Wachtwoord policy's dwingen sterke wachtwoorden af. ▪ Van wachtwoorden wordt alleen een hash opgeslagen incl. een complexe salt.
Encryptie van gegevens	▪ Alle gegevens zijn gedurende transport geëncrypteerd. ▪ Encryptie bij opslag van persoonsgegevens. ▪ Toepassing van tokenization.

Data georiënteerde strategieën	
Afscherming	▪ Strikte toepassing van eigenaarschap. ▪ Rollen- en rechtenbeheer. ▪ Toepassing van het “burgerkluis” principe: alle data die een betrokkene toevoegt aan zijn/haar profiel, wordt automatisch eigendom van die betrokkene en dus *niet* van de werkgever of aanbiedende partij. ▪ Alleen de eigenaar (betrokkene) is in staat tot inzage van essentiële persoonsgegevens. ▪ Persoonsgegevens in de burgerkluis worden standaard met niemand gedeeld. ▪ Eigenaar (betrokkene) bepaalt *welke* data eventueel wel en niet gedeeld wordt, met *wie* en voor *hoe lang*. ▪ Email, verstuurd vanuit het JOHAN Portaal, worden uitsluitend gebruikt als *notificatie* van gereed staande berichten in het JOHAN Portaal. Er wordt geen gevoelige informatie opgenomen in de email berichten zelf. Gebruikers moeten inloggen met hun account om het bericht te kunnen lezen. ▪ De applicatie is privacy-vriendelijk ingericht met betrekking tot http cookies en tracking: er wordt alleen een functioneel cookie geplaats; er zijn geen koppelingen met social media; trackingmechanismes naar derden zijn niet toegestaan; er worden geen persoonsgegevens uitgewisseld die niet behoren tot de gestelde doeleinden (zoals bijv. t.b.v. het aanbieden van gepersonaliseerde advertenties); er wordt geen gebruik gemaakt van analytische software van derden, zoals bijv. Google Analytics; locatiegegevens worden niet opgeslagen.
Transparantie in data	▪ Betrokkene heeft via de eigen account volledig inzicht in de eigen persoonsgegevens. ▪ Betrokkene heeft via de eigen account inzicht in welke data van hem/haar is opgevraagd, door wie die data is opgevraagd, wanneer deze data is opgevraagd en waarom deze data is opgevraagd.
Data minimalisatie	▪ Voor het opzetten van een project door een werkgever, is in beginsel alleen het e-mail adres van de werknemer nodig. ▪ Werknemer wordt aangemoedigd een account aan te maken op zijn / haar privé e-mail adres. ▪ Overige persoonsgegevens worden niet door de werkgever ingevoerd, maar aangevuld door de betrokkene zelf; deze zijn automatisch onderdeel van de burgerkluis. ▪ Ook in overige trajecten is er slechts een minimum aan persoonsgegevens noodzakelijk voor de correcte functionele werking van het JOHAN Portaal.
Granulariteit in de verwerking	▪ Werkgever beheert alleen het zakelijk e-mail adres en een eventueel personeelsnummer

	▪ Werknemer (in rol van burger) beheert de eigen persoonsgegevens (NAWTE e.d.) ▪ Toepassing van datamasking
Scheiding van rollen	▪ Accountactivatie loopt via de betrokkene zelf, niet via de werkgever. De werkgever heeft derhalve geen inzicht in welke werknemers een actieve account in het JOHAN Portaal hebben. ▪ De werkgever heeft geen inzicht in persoonlijke data die de betrokkene toevoegt aan zijn / haar burgerkluis. ▪ De Partner rol heeft beperkte proces inzage m.b.t. de status van werknemers, de werkgever heeft deze inzage niet.
Toestemmingsvereiste bij inzage	▪ Professionals, zoals coaches, kunnen informatie toevoegen aan het persoonlijke profiel van de betrokkene, maar dat kan alleen nadat daar door de betrokkene expliciet toestemming voor is gegeven. Het verlenen van toestemming verloopt via een procedure in het JOHAN Portaal: daarmee is gegarandeerd dat de toestemming ook echt door de betrokkene zelf is gegeven en niet door iemand anders.
Scheiden van gegevens	▪ Persoonsgegevens zijn strikt gescheiden van elkaar, hetgeen op verschillende functionele en technische levels in de applicatie wordt afgedwongen.
Abstraheren en anonimiseren	▪ In reporting komen geen persoonsgegevens voor. ▪ Voor groepsrapportages is een minimaal aantal respondenten noodzakelijk voordat de data getoond kan worden. Data wordt dus alleen getoond indien die onherleidbaar is geanonimiseerd.
Onherleidbaar maken van gegevens	▪ Daar waar het niet strikt noodzakelijk is, worden persoonsgegevens niet of slechts minimaal getoond. ▪ Strikte toepassing van anonimisering bij export van data
Toegangsbeperking	▪ Beperking door rollen- en rechtenbeheer ▪ Beperking in export- en print mogelijkheden
Beperking van opslag	▪ Persoonsgegevens zijn uitsluitend opgeslagen in een datacenter in Nederland. ▪ Persoonsgegevens verlaten onze landsgrenzen niet. ▪ Data is opgeslagen op dedicated servers. ▪ Het datacenter maakt geen gebruik van derden voor opslag, zoals bijv. Amazon Web Services.

Proces georiënteerde strategieën	
Transparantie in proces	▪ Gebruikers worden bij het aanmaken van een JOHAN account geïnformeerd middels een pricvacy-statement, waarin o.a. doel en grondslag van de verwerking is opgenomen. ▪ Gebruikers worden vóór het accepteren van een project of workflow geïnformeerd over de

	gebruikersvoorwaarden van de content / producten in het project of workflow.
Controle geven	▪ Betrokkenen hebben via hun account inzage in hun persoonsgegevens, kunnen deze aanpassen, (laten) verwijderen of meenemen. ▪ Betrokkenen kunnen hun rechten uitoefenen via de supportdesk van JOHAN. ▪ Betrokkenen kunnen een eerder gegeven toestemming voor de inzage van data door een professional intrekken, tenzij er voor die inzage een andere AVG grondslag van toepassing is. ▪ Data portabiliteit is een ingebouwde functie. Een JOHAN account is voor de betrokkene niet gekoppeld aan één werkgever. De betrokkene kan de JOHAN account zolang behouden als hij / zij wenst; data die vanuit één werkgever (aanbieder) is toegevoegd, blijft behouden en kan worden meegenomen naar de volgende werkgever (aanbieder).
Beperking van doorgifte	▪ JOHAN streeft naar een zo klein mogelijk aantal subverwerkers. De belangrijkste is de hostingpartij van de data. ▪ Van iedere subverwerker eist JOHAN dat zij minimaal dezelfde informatiebeveiligings baseline hanteert als JOHAN zelf. ▪ Beperking van gegografische opslag. Opslag en verwerking vindt alleen in NL plaats.
Privacybeleid	▪ JOHAN heeft een directie geïnitieerd en goedgekeurd privacybeleid, dat periodiek wordt gecontroleerd. ▪ Het privacybeleid is gebaseerd op de “*Handleiding Privacy by Design*” en “*de Privacy Baseline*” uitgegeven door het CIP (Centrum Informatiebeveiliging en privacybescherming). ▪ Naleving zoals beschreven in het hoofdstuk “*Eisen vanuit de AVG*”.

6. Aanpak om aan contractuele eisen te voldoen

Contractuele eisen waar JOHAN zich toe verplicht zijn gestandaardiseerd. Zij worden benoemd in de standaard SLA (*Service Level Agreement*) die een integraal onderdeel uitmaakt van de contracten die met klanten en partners worden gesloten. De belangrijkste eisen worden in onderstaande tabel benoemd, waarbij de belangrijkste kernpunten benoemd worden in de aanpak om aan deze eis te voldoen.

Eis	**Aanpak**
Artikel 3 licentieovereenkomst: "*JOHAN is verantwoordelijk voor het technische functioneren van het Platform, voor het functioneren van de daarbinnen door Licentienemer ingekochte functionaliteiten en de beveiliging van het Platform.*"	▪ SSDLC ▪ Hosting in gecertificeerd datacenter ▪ Periodieke PEN test ▪ ISO27001 normering
Privacyverklaring: "*JOHAN is verantwoordelijk voor de privacy waarborging met betrekking tot de Persoonlijke Kluis*"	Bovenstaande plus: ▪ Getoetste privacyverklaring ▪ Informed consent
Beschikbaarheid van het Portaal: 99,9%	Bovenstaande plus: ▪ SLA met hostingpartij ▪ Periodieke SLA rapportage ▪ Procedure voor opzetten productie-omgeving ▪ Backup- en restore procedures
Verwerkersovereenkomst: "*JOHAN heeft passende technische en organisatorische beveiligingsmaatregelen getroffen om veilig gebruik van het Platform te waarborgen conform de toepasselijke Wet- en regelgeving met betrekking tot privacy, waaronder de AVG*"	Bovenstaande plus: ▪ Vastgesteld IB beleid ▪ Aanstelling security officer ▪ Privacy-by-design ▪ Privacy-by-default ▪ Security-by-design ▪ **ISO27001:2017 certificering** ▪ Periodieke PIA
Artikel 4 SLA: Responsetijden bij incidenten waarborgen, onder incidentlevel 1 t/m 4 (zie SLA)	Bovenstaande plus: ▪ Wijzigingsprocedure ▪ Incidentmanagement ▪ Ticketsysteem ▪ Supportteam vanuit hostingpartij, 24x7 ▪ Supportteam vanuit Johan, 8x5 ▪ Continuous development
Artikel 5 SLA: Ondersteuning bij implementatie	▪ Implementatie team ▪ Support website ▪ Periodieke nieuwsbrieven

NB: Bovenstaande aanpak is uitgewerkt in het Information Security Management System (ISMS) van JOHAN. Grote delen van de bijbehorende documenten zijn ofwel openbaar (zoals de Verklaring van Toepasselijkheid) of worden op verzoek ter inzage gegeven, bijvoorbeeld als onderdeel van een audit.

7. Aanpak om aan eisen vanuit de AVG te voldoen

De belangrijkste wettelijke eisen m.b.t. informatiebeveiliging (IB) en borging van privacy zijn vastgelegd in de AVG en de bijbehorende uitvoeringswet. Onderstaande tabel noemt de belangrijkste op. De aanpak van de eisen die de AVG stelt, kan niet los worden gezien van de IB aanpak die JOHAN reeds volgt naar aanleiding van de contractuele eisen, zoals hierboven is beschreven. Bescherming van privacy is immers onmogelijk zonder een effectief en toepasselijk IB beleid. Vrijwel de volledige bovenstaande IB aanpak is daarom integraal van toepassing op onderstaande.

Eis	**Aanpak**
Bijhouden verwerkingsregister	▪ Document wordt periodiek geactualiseerd door de privacy officer
Opstellen beveiligingsbeleid	▪ Directie geïnitieerd en gecontroleerd ▪ Aanstelling security officer ▪ Aanpak conform ISO27001:2017
Het documenteren van gegevensbeschermings-effectbeoordelingen	▪ Periodieke PEN testen ▪ Security- en PIA audits vanuit prospects of klanten ▪ Door JOHAN uitgevoerde PIA ▪ Interne en externe ISO27001 audit
Documenteren van passende waarborgen die worden gehanteerd bij de overdracht van gegevens buiten de Europese Unie	▪ Data-opslag beperken tot NL ▪ Verklaring van beperking van geografische opslag ▪ Geen doorgifte naar landen zonder adequaatheidsbeslissing ▪ Alleen doorgifte aan partijen die voldoen aan door de Europese Commissie of AP goedgekeurde standaard contractbepalingen (SCC) ▪ Doorgifte beperken tot kortstondige verwerking van het e-mail adres van de accounthouder t.b.v. het kunnen afhandelen van e-mail berichten
Informatievoorziening aan de betrokkenen op schrift stellen	▪ Getoetste privacyverklaring ▪ Gebruikersvoorwaarden
Grondslag “Toestemming betrokkene“	▪ Expliciete Informed consent bij activeren van een Johan account ▪ Expliciete Informed consent bij afname van content via het Johan Portaal ▪ Vastlegging van deze toestemming d.m.v. logging
Verwerkersovereenkomst	▪ JOHAN is verwerkingsverantwoordelijke voor de “burgerkluis”. Voorwaarden verankert in privacyverklaring en gebruikersvoorwaarden ▪ JOHAN is (sub)verwerker voor de werknemers data zoals die door partners en/of werkgevers in het JOHAN Portaal geladen wordt ▪ Verwerkersovereenkomst voor partners / klanten maakt integraal onderdeel uit van het contract met de klant. Deze wordt digitaal ondertekend bij het aangaan van een contract ▪ Verwerkersovereenkomst met alle subverwerkers, waaronder de hosting leverancier ▪ Periodieke controle op actualiteit

Meldplicht datalek AP	▪ Beschreven in procedure datalek
Implementeren van beveiligingsmaatregelen	Bovenstaande plus: ▪ VVT ISO27001:2017
Invulling geven aan de uitgangspunten van gegevensbescherming door ontwerp en door standaardinstellingen	Zie paragraaf “Toepassing Privacy by design en Privacy by default”
Documenteren van processen en procedures ter waarborging van de rechten van de betrokkenen	▪ Betrokkene is eigenaar van de eigen data (“burgerkluis”) en kan die data via de account inzien, muteren, (laten) verwijderen en overdragen ▪ Uitoefening van rechten via bovenbeschreven “self-service” of via supportdesk JOHAN ▪ Beperking op geautomatiseerde besluitvorming en profilering
Aantoonbaar voldoen aan de AVG	Bovenstaande plus: ▪ aanstelling van een privacy officer. (Zie ook de specifieke taken hieronder)

De security- en privacy officer:

- adviseert de directie inz. IB- en privacy-beleid;
- rapporteert periodiek over de uitvoering van zijn taken aan de directie;
- stelt de interne norm vast waar de organisatie aan wenst te voldoen m.b.t. IB en privacy;
- zorgt voor voldoende awareness onder de medewerkers van JOHAN door middel van IB- en privacy trainingen;
- is actief betrokken bij de ontwikkeling van het JOHAN Portaal en borgt de toepassing van security-by-design en privacy-by-design principes;
- beoordeelt periodiek of het ISMS werkt en ziet toe op naleving van de genomen maatregelen;
- is verantwoordelijk voor het bijhouden van het verbeterplan en bewaakt de voortgang hiervan;
- is verantwoordelijk voor het (laten) uitvoeren van impact analyses, PEN testen en PIA’s c.q. gegevensbeschermingseffectbeoordelingen;
- informeert en adviseert de directie over verplichtingen op grond van de AVG en andere toepasselijke wetgeving;
- houdt zich op de hoogte van de ontwikkelingen door zich o.a. te abonneren op relevante fora of kennisgroepen;
- controleert periodiek of er wijzigingen zijn in de AVG of de uitvoeringswet daarvan;
- controleert de relevantie van andere wettelijke eisen n.a.v. wijzigingen in organisatie of beleid;
- treedt op als contactpersoon richting AP.