



Easyflex en de AVG

Whitepaper mei 2018

Inleiding

Vanaf 25 mei 2018 geldt nog maar één privacywet in de hele EU: de algemene verordening gegevensbescherming (AVG). De Wet Bescherming Persoonsgegevens komt hiermee te vervallen. Het uitgangspunt van de AVG is dat persoonsgegevens alleen mogen worden verwerkt wanneer dat strikt noodzakelijk is. Bij overtreding van deze wet kunnen organisaties sancties opgelegd krijgen.

In deze whitepaper tref je een weergave van de eisen die de AVG met zich meebrengt en een aantal tips & tricks hoe je aan de AVG kunt voldoen door middel van functionaliteiten in Easyflex.

Bronnen:

De [Autoriteit Persoonsgegevens](#), [ABU](#), [HR Kiosk](#)

Dit whitepaper geeft een globaal beeld van jouw privacyverplichtingen, maar bevat uitdrukkelijk geen juridisch advies. Dit whitepaper is niet juridisch bindend, noch kunnen hier rechten aan worden ontleend of kan hier enige aansprakelijkheid of verplichting voor Easyflex uit voortvloeien.

Inhoudsopgave

1. Persoonsgegevens
2. Documentatieplicht
3. Dataportabiliteit
4. Verlenen van toestemming
5. Vastleggen van gezondheidsgegevens
6. Beveiliging
7. Samenvattend: Stappen voor de AVG

Bijlage 1 Tips & Tricks

1. Two-factor Authentication
2. Notificaties
3. Memovelden
4. Toegangstijden afschermen
5. IP-filters
6. Documenten verwijderen
7. Autorisaties vastleggen
8. Dataportabiliteit

1. Persoonsgegevens

1.1 Wat zijn persoonsgegevens?

Alle gegevens waarmee je een natuurlijk persoon kunt identificeren. Hieronder vallen: NAW-gegevens, e-mailadressen, telefoonnummers, personeelsnummers, geboortedata, geslacht, nationaliteit, werkervaring en opleidingen, IP-adressen, logingegevens etc.

1.2 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens waaruit iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, gezondheid, strafrechtelijk gedrag, seksuele leven of het lidmaatschap van een vakbond blijken. Ook genetische gegevens en biometrische gegevens voor unieke identificatie van een persoon vallen hieronder.

Voorbeelden hoe je hier als flexbedrijf mee te maken kunt krijgen:

- Godsdienstgegevens (of een uitzendkracht/kandidaat een hoofddoek draagt) mogen niet worden verwerkt. Zelfs niet als een uitzendkracht werkzaam is.
- Gezondheidsgegevens (zoals over aandoeningen, verzuim, handicap en beperkingen) mogen niet worden verwerkt. Tenzij dit noodzakelijk is ter bescherming van een belang dat voor het leven van de betrokkene essentieel is (een vitaal belang). Bijvoorbeeld bij ernstige epilepsie.

Bijzondere persoonsgegevens mogen in principe nooit verwerkt worden, tenzij een wettelijke uitzondering van toepassing is en het strikt noodzakelijk is om ze hiervoor te verwerken. Voor meer informatie hierover verwijzen we je naar de website van de Autoriteit Persoonsgegevens.

1.3 Bewaartermijnen

In het schema [Bewaartermijnen](#) vind je de verschillende categorieën gegevens, hoe lang ze bewaard mogen worden en waar de richtlijnen daarvoor vastliggen. Indien noodzakelijk en legitiem mogen gegevens mogelijk langer bewaard worden, bijvoorbeeld als ze noodzakelijk zijn voor de afhandeling van een concrete klacht of claim. Let op: De gegevens moeten in ieder geval op verzoek van de uitzendkracht/kandidaat worden verwijderd!

1.4 BSN en kopie-identiteitsbewijs

- In geval van bemiddeling:
Sinds 1 januari 2018 mag je ook een kopie van het identiteitsdocument in je administratie bewaren van een werkzoekende die nog niet aan een opdrachtgever ter beschikking is gesteld, maar daar wel voor in aanmerking komt. Je mag de gegevens die op de kopie van het identiteitsbewijs staan alleen niet afzonderlijk registreren.
Een uitzondering hierop is het BSN voor het nagaan bij UWV of iemand in het doelgroepregister vermeld staat. Hierover moet de ingeschreven uitzendkracht wel worden geïnformeerd. En na deze toetsing moet het BSN weer verwijderd worden. Voor de pasfoto geldt dat deze wel afzonderlijk verwerkt mag worden als de uitzendkracht hiervoor uitdrukkelijk toestemming heeft gegeven en hierover voldoende is geïnformeerd.
- In geval van (uitzend)overeenkomst:
Als er een (uitzend)overeenkomst met de uitzendkracht wordt aangegaan, mag een uitzendonderneming het BSN van de uitzendkracht verwerken voor specifieke doelen (zie hieronder). Het BSN moet voor aanvang van de werkzaamheden in de administratie zijn opgenomen.

1.5 Waarvoor mag je het BSN verwerken?

- Voor het uitvoeren van de (inhoudingen) loonbelasting en de salaris- en pensioenadministratie (inclusief loonaangifte bij de Belastingdienst).
- Om de identiteit van de uitzendkracht vast te stellen.
- Als je eigenrisicodragers bent volgens de Ziektewet.
- Bij gegevensverstrekking aan UWV in verband met ziekte en re-integratie.
- Bij verstrekking aan de bedrijfsarts in het kader van re-integratie van de uitzendkracht.
- Ten behoeve van een aanvraag over vermelding in het doelgroepregister van UWV.

1.6 Verwerken gegevens Loonbeslag

- Je mag alleen gegevens verwerken als er een loonbeslag is vastgelegd en alleen voor zover dat noodzakelijk is voor de salarisadministratie en uitvoer van het loonbeslag.
- Alleen medewerkers voor wie het noodzakelijk is voor hun werk, mogen toegang hebben tot gegevens over het loonbeslag.
- Wanneer het loonbeslag wordt opgeheven, mogen deze gegevens niet langer worden bewaard.

2. Documentatieplicht

2.1 Dataverwerkingsregister

Binnen de flexbranche worden heel veel persoonsgegevens verwerkt en opgeslagen. Vanaf 25 mei is het van belang dat je van je eigen organisatie inzichtelijk hebt waar deze gegevens verwerkt en opgeslagen worden. Dit moet namelijk intern geregistreerd worden in een dataverwerkingsregister.

Wat moet er allemaal opgenomen worden in dit register?

- De naam en contactgegevens van de functionaris voor gegevensbescherming. Op de website van de autoriteit persoonsgegevens kun je nagaan of het aanstellen van een functionaris voor gegevensbescherming voor jouw organisatie verplicht is. (bv. bedrijven in de private sector met meer dan 250 medewerkers; bedrijven in de private sector met als core business het regulier volgen van individuen; overheidsdiensten.)
- De doeleinden waarvoor gegevens worden verwerkt (per gegevenstype)
- De categorie gegevens (NAW-gegevens, contactgegevens, betaalgegevens)
- De categorie betrokkenen (klanten, werknemers etc.)
- De categorie ontvangers (aan wie worden de gegevens verstrekt)
- Informatie over het eventueel doorgeven van deze gegevens naar landen buiten de EU
- De (voorgenomen) bewaartermijn van deze gegevens
- De manieren waarop deze gegevens zijn beveiligd

Het is belangrijk dat het register schriftelijk opgesteld wordt en actueel blijft. Zorg er dus voor dat dit register regelmatig *gereviewd* wordt en deze makkelijk aan te passen is.

2.2 Privacyverklaring

Organisaties die persoonsgegevens verwerken, moeten heldere informatie geven over de persoonsgegevens die verwerkt worden en de doelen daarvan. Dit kan gedaan worden door online een privacyverklaring op te stellen. Op deze manier is de informatie voor iedereen transparant en inzichtelijk.

In de AVG staat niet precies omschreven welke gegevens in de privacyverklaring opgenomen moeten worden. Het is vooral belangrijk dat uit deze verklaring blijkt hoe jouw organisatie voldoet aan de AVG, dit is namelijk onderdeel van de verantwoordingsplicht. Veel van deze informatie zal ook al terugkomen in het dataverwerkingsregister. Zorg er dus voor dat je geen dubbel werk doet en stem deze informatie op elkaar af.

Om aan te tonen dat jouw organisatie aan de verantwoordingsplicht voldoet kan je de volgende informatie opnemen in je privacyverklaring:

- Omschrijving van de categorieën persoonsgegevens die door jouw organisatie verwerkt worden
- Een beschrijving van de doeleinden waarvoor de persoonsgegevens verwerkt worden en de juridische grondslag daarvan
- Hoe jouw organisatie voldoet aan de beginselen van de verwerking van persoonsgegevens. Geef hierbij dus aan dat er niet meer gegevens verwerkt worden dan noodzakelijk
- Welke rechten betrokkenen hebben en hoe deze uitgeoefend kunnen worden. Denk hierbij aan het recht op inzage, wijzigen en wissen en ontvangen van de geregistreerde gegevens
- Welke organisatorische en technische maatregelen jouw organisatie genomen heeft om de persoonsgegevens te beveiligen
- Hoe lang persoonsgegevens bewaard worden

3. Dataportabiliteit

Artikel 20 van de AVG introduceert per 25 mei een nieuw recht: het recht op dataportabiliteit. Simpel gezegd houdt dit in dat een betrokkene recht heeft op de overdraagbaarheid van gegevens. De betrokkene heeft dus het recht om zijn/haar persoonsgegevens, die zijn verstrekt aan een organisatie, zo snel mogelijk (in een machine leesbare vorm) te ontvangen. Dit kan bijvoorbeeld een print cv zijn of een export van alle gegevens in een CSV bestand. Let op: dit geldt uitsluitend voor digitale gegevens, papieren dossiers vallen hier dus niet onder. Na een verzoek voor dataportabiliteit hoeven de gegevens niet verwijderd te worden zolang de betrokkene hier niet expliciet om vraagt. Betrokkenen kunnen deze persoonsgegevens vervolgens opslaan voor persoonlijk (her)gebruik of doorgeven aan een andere organisatie. De organisatie draagt geen verantwoordelijkheid voor het verdere gebruik van de gegevens na het overdragen van de gegevens.

3.1 Recht op inzage en dataportabiliteit

Naast het recht op overdraagbaarheid van gegevens is er ook het recht op inzage. Dit kan verwarrend zijn en de verschillen zijn wellicht nog niet helemaal duidelijk. Het verschil zit hem in de verplichting van de organisatie. Bij het inzagerecht mag een betrokkene aan een organisatie vragen om inzage te krijgen in zijn/haar persoonsgegevens. Echter, kunnen organisaties zélf beslissen hoe zij de gegevens ter inzage geven. Een voorbeeld: een flexwerker maakt gebruik van het inzagerecht door aan te geven zijn persoonsgegevens die de organisatie verwerkt, te willen inzien. De organisatie mag dan zelf bepalen op welke manier de flexwerker inzicht krijgt in zijn gegevens. Zij kunnen er bijvoorbeeld voor kiezen om de flexwerker op kantoor uit te nodigen om zijn gegevens te komen inzien. Dit hoeft dus niet altijd aangeleverd te worden middels een digitaal personeelsdossier. Bij het recht op dataportabiliteit is dit anders. Hierbij is de organisatie verplicht gegevens te verstrekken in een machine leesbare vorm die de betrokkene gemakkelijk kan (her)gebruiken voor persoonlijke doeleinden of om door te geven aan een andere organisatie.

3.2 Welke gegevens moet ik verstrekken?

Het antwoord daarop is vrij simpel: álle persoonsgegevens moeten beschikbaar worden besteld. Let op: dit geldt niet alleen voor persoonsgegevens die de betrokkene bewust heeft verstrekt (bijv. telefoonnummer, e-mailadres, leeftijd) maar ook de gegevens die onbewust zijn verstrekt (bijv. zoekgeschiedenis, locatiegegevens). De gegevens die zijn afgeleid van deze data, dus bijvoorbeeld een klantprofiel/rating wat is gemaakt n.a.v. de persoonsgegevens door de organisatie, hoeven niet verstrekt te worden.

3.3 Binnen welke termijn moet je reageren op een verzoek van dataportabiliteit?

In principe zo snel mogelijk, al is dit een vrij vaag begrip. De AVG houdt hier één maand aan, tenzij het een complex verzoek is, dan bedraagt de termijn drie maanden. Een verzoek kan ook geweigerd worden, al moet je dit wel binnen één maand laten weten met een reden waarom het verzoek is geweigerd.

4. Verlenen van toestemming

In de AVG is er extra aandacht voor de manier waarop toestemming wordt verleend door de flexwerker of relatie voor de verwerking van de persoonsgegevens.

4.1 Duidelijk en vrijwillig toestemming geven

Het is belangrijk dat er een 'duidelijke actieve handeling' door de flexwerker wordt gedaan. Toestemming vragen door middel van een vooraf aangevinkt vinkje is bijvoorbeeld niet toegestaan. Ook moet de toestemming 'ondubbelzinnig' zijn, dus een onduidelijke vraag of een toestemmingsvraag opnemen ergens ver weg in een contract is niet voldoende. Om aan de wet te voldoen moet het direct duidelijk zijn voor de flexwerker dat én waarvoor hij met die handeling toestemming geeft voor het verwerken van zijn gegevens. Maak dit dus zo duidelijk en eenvoudig mogelijk.

Een ander punt om rekening mee te houden is dat de toestemming 'vrij' moet zijn. Het is niet toegestaan om toestemming te vereisen bij het aangaan van een overeenkomst, tenzij alle gegevens perse nodig zijn voor de uitvoering van die overeenkomst. Concreet moet je als uitzendonderneming vooral goed kijken welke gegevens je écht nodig hebt en dit geldt zowel voor flexwerkers als relaties.

4.2 Specifiek per doeleinde vastleggen en intrekken

Let erop dat je specifiek aangeeft welke gegevens er gebruikt worden en wat de reden daarvan is. Algemene vermeldingen zijn niet toegestaan, het is belangrijk dat de flexwerker of relatie exact weet welke persoonsgegevens je gaat verwerken en waarom. Je moet als organisatie kunnen aantonen dat er toestemming is verleend en waarvoor dit is gedaan. Daar moet je het bedrijfsproces op inrichten. Zorg dat je de vraag altijd juist stelt en leg het antwoord vast.

Houdt daarbij rekening dat de flexwerker of relatie de toestemming altijd kan intrekken. Dit moet net zo eenvoudig zijn als de manier waarop de toestemming is verleend. Zorg ervoor dat er een proces is dat je kunt volgen om deze verzoeken te kunnen inwilligen. Wel is het zo dat er toestemming verleend (en dus ook ingetrokken) wordt voor een specifieke verwerking (denk aan de nieuwsbrief). Verwijder je op verzoek het e-mailadres van de mailinglijst, wil dat niet zeggen dat je het volledig uit je klantenbestand moet wissen. Voor die verwerking is namelijk in dit voorbeeld apart toestemming gegeven.

5. Vastleggen van gezondheidsgegevens

Voor het vastleggen van 'gezondheidsgegevens' van flexwerkers in de administratie van de werkgever zijn er in de AVG verschillende bepalingen opgenomen. Deze verschillen weinig van de voorheen geldende bepalingen in de WBP, dus in de uitvoering zal hier weinig veranderen. Wel is het goed om deze punten nog eens goed onder de aandacht te brengen binnen de organisatie, zodat alle medewerkers op de hoogte zijn wat er wel en niet mag worden vastgelegd.

In artikel 6 AVG staat omschreven dat voor het vastleggen van gezondheidsgegevens (dus ziekte / verzuim) een wettelijke grondslag aanwezig moet zijn. Ook moet je aan de overige eisen van de AVG hebben voldaan, en moet de flexwerker zich eventueel kunnen beroepen op het verbieden van bijzondere categorieën persoonsgegevens (deze zijn eerder toegelicht).

Omdat werkgevers verplicht zijn een ziekmelding op te nemen in hun administratie in het kader van de loondoorbetalingsverplichting, is het hierbij belangrijk dat je deze informatie beperkt tot enkel datgene wat noodzakelijk is. De medische achtergrond, of reden dat de flexwerker ziek is wordt in de AVG (en ook in de Wpb) niet gezien als noodzakelijk, dus deze mag je niet registreren. Let erop dat er ook geen notitie of notificatie vastligt met deze informatie.

5.1 Welke gegevens mogen wel geregistreerd worden bij ziekmelding?

- Het telefoonnummer en (verpleeg)adres, zolang de ziekte daaruit niet herleidbaar is.
- De vermoedelijke duur van het verzuim.
- Lopende afspraken en werkzaamheden.
- Of de werknemer valt onder een van de vangnetbepalingen van de Ziektewet. Dit is na twee maanden dienstverband toegestaan. Er mag niet worden gevraagd onder welke vangnetbepaling de werknemer valt.
- Of de ziekte verband houdt met een arbeidsongeval.
- Of sprake is van een verkeersongeval met verhaalsmogelijkheid.

Let op: overige gezondheidsgegevens mogen **niet** verzameld of verder verwerkt worden, omdat die niet noodzakelijk zijn voor de loondoorbetalingsverplichtingen of re-integratie. Zij vallen onder het medisch beroepsgeheim. De bedrijfsarts mag deze gegevens van de uitzendkracht dus ook niet aan de uitzendonderneming verstrekken.

5.2 Welke gegevens mogen niet worden verwerkt?

- De aard en oorzaak van verzuim, waaronder de naam van ziekten en specifieke klachten. Het is voldoende om kennis te hebben van functionele beperkingen: wat de uitzendkracht wel en niet kan.
- Eigen subjectieve waarnemingen over de geestelijke of lichamelijke gezondheidstoestand van de uitzendkracht.
- Of een ziekte werkgerelateerd is of bijvoorbeeld te maken heeft met relatieproblemen.
- Gegevens over therapieën, afspraken met artsen, fysiotherapeuten, psychologen.

Let op: ook wanneer een uitzendkracht vrijwillig informatie geeft over de aard en oorzaak van het ziekteverzuim, mogen deze gegevens niet worden vastgelegd. Dit mag alleen als het noodzakelijk is ter bescherming van een belang dat voor het leven van de betrokkene essentieel is (dit is een vitaal belang).

6. Beveiliging

Easyflex heeft het afgelopen jaar een aantal grote wijzigingen op het gebied van informatiebeveiliging doorgevoerd. Deze stappen zijn gemaakt in het licht van de AVG, waarin hoge eisen worden gesteld op het gebied van informatiebeveiliging.

6.1 ISO 27001

Veilig databeheer en -beleid zijn van groot belang zowel in Nederland als internationaal. Begin 2018 heeft Easyflex het ISO 27001:2013 certificaat ontvangen. Natuurlijk benaderden wij in het verleden data ook al volgens strenge normen, heldere procedures en duidelijke werkafspraken, want veilig omgaan met informatie is altijd al een onlosmakelijk onderdeel van onze dienstverlening. Met het behalen van de certificering heeft dit alles nu een officieel en internationaal erkend keurmerk gekregen. Hoewel ISO 27001:2013 certificering niet vereist is in de softwarebranche, vinden wij het belangrijk dat alle vertrouwelijke gegevens nóg veiliger behandeld worden en dit ook met regelmaat aangetoond wordt.

6.2 Two-factor Authentication

Easyflex heeft two-factor authentication in de software gebouwd om het inloggen en werken nóg veiliger te maken. Het gebruik van tfa creëert een extra beveiligingslaag in Easyflex. De gebruiker logt in met zijn gebruikelijke wachtwoord én ontvangt daarnaast via de Google Authenticator app voor elke nieuwe inloggoging een unieke code die nodig is om te kunnen inloggen. Deze extra beveiliging is een grote stap ten behoeve van de AVG.

6.3 Easyflex Connector

In het kader van beveiliging heeft Easyflex ook de ActiveX vervangen, het stukje software dat nu nodig is om Easyflex in een browser te draaien. Dit wordt vervangen door de Easyflex Connector. Ook deze stap is ondernomen om het inloggen en werken met Easyflex nóg veiliger te maken. De Easyflex Connector installeer je als programma op je pc en wanneer je deze opent middels een icoon op je bureaublad, wordt Easyflex automatisch opgestart. De Connector heeft nog wel een Windows-omgeving en een werkende internetverbinding nodig om op te draaien. Ook worden je gebruikersnaam en bedrijfsnaam niet meer onthouden.

6.4 Service Center

Onlangs is de werkwijze op het Service Center aangepast. In het verleden keken we met onze klanten mee in hun eigen omgeving, maar in het kader van de informatiebeveiliging en de AVG is besloten om dit aan te passen. Vanaf nu heeft het Service Center niet meer de mogelijkheid om met je mee te kijken in je eigen actuele data, maar kunnen we uitsluitend met je meekijken via schermdeling. Je kunt op <https://www.easyflex.nl/downloads> of in het handboek het programma Teamviewer downloaden.

Uiteraard hebben we in geanonimiseerde testschema's nog steeds de mogelijkheid om bepaalde functionaliteiten te testen/controleren.

6.5 Verwerkersovereenkomst, ALV en SLA

Op onze website vind je altijd onze meest recente Algemene Leveringsvoorwaarden (ALV), Service Level Agreement (SLA) en de verwerkersovereenkomst. Ga naar <https://www.easyflex.nl/gebruikersvoorwaarden>.

7. Samenvattend: Stappen voor de AVG

Deze stappen adviseren wij met het oog op de AVG:

- Lees of bekijk de tips en tricks die Easyflex uitbrengt over hoe je aan je verplichtingen kunt voldoen binnen Easyflex.
- Breng het gebruik van persoonsgegevens binnen jouw organisatie in kaart. Letterlijk: welke gegevensstromen of administraties zijn er? Personeelsgegevens, klantgegevens, gegevens van sollicitanten of deelnemers?
- Heb je voor bepaalde verwerking/gebruik van deze gegevens toestemming nodig volgens deze regels? Pas dan waar nodig je interne processen aan.
- Houd alle gegevensverwerking bij in een dataregister.
- Check of je voldoet aan de documentatieplicht.
- Loop de bewaartermijnen door en pas je interne processen hier waar nodig op aan.
- Voer een privacybeleid in waarmee je inzichtelijk maakt hoe je omgaat met alle persoonsgegevens die binnen jouw organisatie worden gebruikt, gedeeld en bewaard.
- Check of je verplicht bent om een privacyfunctionaris aan te stellen en zo ja, zet hiervoor de benodigde stappen.

Bijlage 1 Tips & Tricks

Ben jij al AVG-proof? Easyflex helpt je verder op weg!

De Algemene verordening gegevensbescherming (AVG) is een *hot topic* in uitzendland. De AVG vervangt met ingang van 25 mei 2018 de Wet bescherming persoonsgegevens (Wbp). Wij begrijpen dat dit de nodige veranderingen teweeg brengt en helpen je daarom graag verder om de juiste aanpassingen door te voeren conform de AVG. Wij hebben een lijst opgesteld met handige *tips en tricks* die je kunt gebruiken in Easyflex.

1. Two-factor authentication

Easyflex heeft two-factor authentication (tfa) toegevoegd aan de software. Deze stap is ondernomen om het inloggen en werken met Easyflex nóg veiliger te maken. Het gebruik van tfa creëert een extra beveiligingslaag in Easyflex en hiermee beperk je het risico dat je inloggegevens in verkeerde handen vallen. De gebruiker logt in met zijn gebruikelijke wachtwoord én ontvangt daarnaast via de Google Authenticator app voor elke nieuwe inlogpoging een unieke code die nodig is om te kunnen inloggen. Deze extra beveiliging is een grote stap ten behoeve van de AVG.

Connector

Wij adviseren om two-factor authentication te gebruiken in combinatie met de Connector, samen vormen deze de meest veilige manier van inloggen. Met het gebruik van de Connector ben je ook niet gebonden aan het gebruik van de Internet Explorer browser. De Connector kun je downloaden op de website: www.easyflex.nl/downloads. Volg de stappen om de installatie te voltooien. De Easyflex Connector zal nu als icoontje op jouw bureaublad komen te staan. Vanaf nu kan je via dit icoontje inloggen in Easyflex.

Hoe werkt het?

Het gebruik van tfa is optioneel en wordt vastgelegd op werkmaatschappij niveau. Zodra het geactiveerd wordt, geldt het dus voor alle medewerkers. Bij 'Beheer > Inlogbeleid' kun je aanvinken of je hier gebruik van wilt maken. Vanaf het moment dat je het activeert, moeten alle gebruikers inloggen met een extra inlogcode.

Eerste keer inloggen, ik heb de Google Authenticator app nog niet op mijn telefoon

- Download eerst de Google Authenticator app uit de App Store of Google Play Store.
- Open de app en kies voor 'Starten'. Je komt dan bij het onderdeel 'Een account toevoegen'. Klik dan op 'Een streepjescode scannen'.
- Log in bij de Easyflex applicatie met je gebruikersnaam/e-mailadres, bedrijfsnaam en wachtwoord. In het volgende scherm wordt automatisch een QR-code getoond. Scan deze code met de Google Authenticator app. Je account is nu geactiveerd.
- Vervolgens verschijnt in de app een unieke code die je invult bij het veld 'Authenticatiecode' en klik op 'Inloggen'. Je bent nu ingelogd in Easyflex!

Eerste keer inloggen, maar ik heb de Google Authenticator app al op mijn telefoon

- Open de Google Authenticator app en selecteer het rode icoontje met het plus (+) teken om een account toe te voegen. Kies daarna voor 'Een streepjescode scannen'.
- Log in bij de Easyflex applicatie met je gebruikersnaam/e-mailadres, bedrijfsnaam en wachtwoord. In het volgende scherm wordt automatisch een QR-code getoond. Scan deze code met de Google Authenticator app. Je account is nu geactiveerd.
- Vervolgens verschijnt in de app een code die je invult in het veld 'Authenticatiecode' en klik op 'Inloggen'. Je bent nu ingelogd in Easyflex!

Volgende keren inloggen

Elke volgende keer dat je inlogt, open je direct de Google Authenticator app. Bij het account dat gekoppeld is aan Easyflex verschijnt nu automatisch een unieke inlogcode. Deze vul je in tijdens het inlogproces in het veld 'Authenticatiecode'. Dit doe je pas ná het invullen van je gebruikersnaam/e-mailadres, bedrijfsnaam en wachtwoord.

Smartphone niet bij de hand?

De eerste keer dat je als gebruiker inlogt met two-factor authentication krijg je een melding te zien dat er back-upcodes gegenereerd moeten worden. Dit zijn codes die je kunt gebruiken als alternatief voor de inlogcodes die de app genereert. Heb je je smartphone dus niet bij de hand en wil je toch kunnen inloggen? Zorg dan dat je altijd de back-upcodes bij de hand hebt. Je genereert een overzicht met 10 back-upcodes in 'Mijn gegevens > Back-upmethode'. Elke back-upcode kan slechts éénmalig gebruikt worden. Zodra je nieuwe back-upcodes genereert, komen de vorige te vervallen.

Een medewerker resetten

Het kan nodig zijn om een medewerker te resetten. Bijvoorbeeld als je een nieuwe smartphone hebt. Ga naar 'Beheer > Medewerkers', selecteer de betreffende medewerker en ga naar het tabblad 'Licenties'. Hier zie je rechtsbovenin de optie 'Two-factor authentication-koppeling' en de knop 'Reset'. Klik op de knop 'Reset'. De medewerker kan zichzelf nu opnieuw koppelen door met de Google Authenticator app de QR-code te scannen.

In 'Beheer > Bedrijfsinstellingen > Inlogbeleid' kun je een rol vastleggen voor het mogen resetten van de koppeling. Leg je hier geen rol vast? Dan mogen alle medewerkers (die toegang hebben tot 'Beheer > Medewerkers > Licenties') een gebruiker resetten.

2. Notificaties

Vanuit de regelgeving van de AVG is het niet toegestaan om zomaar allerlei gegevens vast te leggen van een flexwerker. Zo is het bijvoorbeeld niet toegestaan om vast te leggen welke ziekte iemand heeft als diegene zich ziek heeft gemeld. Wellicht had je er nog niet aan gedacht, maar soms liggen dit soort gegevens vast als notificatie in Easyflex.

Wil je weten wat er nu als notificatie vastligt? Je kunt daar eenvoudig een overzicht voor draaien:

- Ga naar 'Backoffice > Overzichten' en kies vervolgens het overzicht 'Acties en notificaties'.
- Je kunt hier kiezen voor 'handmatige notificaties', 'automatische notificaties' of beide. De handmatige notificaties zijn bijvoorbeeld de notificaties die zijn vastgelegd bij een flexwerker door een interne medewerker. Automatische notificaties zijn bijvoorbeeld gegevens die zijn aangepast in de plaatsing door een interne medewerker, dit wordt automatisch gelogd door Easyflex.
- Selecteer hier vervolgens een bepaalde periode om alle notificaties en acties te bekijken.
- Je kunt instellen dat dit overzicht standaard (bijvoorbeeld elke maand) gedraaid wordt. Dit doe je onder het kopje 'Uitvoeren > Wanneer verwerken?'. Deze staat standaard op 'Direct', pas dit bijvoorbeeld aan naar 'Eind van elke maand'. Je kunt dit overzicht ook automatisch naar jezelf laten mailen wanneer deze wordt aangemaakt. Dit doe je door op de drie puntjes te klikken achter 'Gereed melden aan'. Kies hier voor 'nieuw' en vervolgens voor 'e-mail' onder type berichtgeving.
- Aan de hand van het overzicht kun je handmatig de notificaties en acties verwijderen die niet vastgelegd mogen worden.

3. Memovelden

Naast Notificaties, worden ook Memovelden wel eens gebruikt om (extra) gegevens vast te leggen. Wellicht heb je gegevens vastgelegd in de memovelden, bijvoorbeeld dat een flexwerker een hoofddoek draagt, wat niet meer toegestaan is. Om snel terug te vinden welke informatie er in de memovelden vastligt, voer je bijna dezelfde stappen uit zoals hierboven beschreven zijn:

- Ga naar 'Backoffice > Overzichten' en kies vervolgens het overzicht 'Memovelden'.
- Selecteer hier alle memobladen waar je op wil filteren.
- Je kunt instellen dat dit overzicht standaard (bijvoorbeeld elke maand) gedraaid wordt. Dit doe je onder het kopje 'Uitvoeren > Wanneer verwerken?'. Deze staat standaard op 'Direct', pas dit bijvoorbeeld aan naar 'Eind van elke maand'. Je kunt dit overzicht ook automatisch naar jezelf laten mailen wanneer deze wordt aangemaakt. Dit doe je door op de drie puntjes te klikken achter 'Gereed melden aan'. Kies hier voor 'nieuw' en vervolgens voor 'e-mail' onder type berichtgeving.
- Aan de hand van het overzicht kun je handmatig de memovelden verwijderen die niet vastgelegd mogen worden.

4. Toegangstijden afschermen

In Easyflex kun je de toegangstijden voor gebruikers limiteren. Daarmee zorg je ervoor dat gebruikers niet buiten kantooruren kunnen inloggen. Je beperkt hiermee voor een deel de beveiligingsrisico's doordat niemand buiten deze vooraf ingestelde tijden kan inloggen. Dit doe je als volgt:

- Ga naar 'Beheer > Bedrijfsinstellingen > Toegangstijden'.
- Hier kun je naar wens de geldende werktijden per werkmaatschappij instellen. Let op: degene met de beheerdersrol in Easyflex heeft ongeacht alle instellingen wél altijd toegang tot Easyflex binnen de contractueel overeengekomen toegangstijden (eerste uitgedrukte kolom).
- Je kunt er ook voor kiezen dat gebruikers na een X aantal minuten uitgelogd worden als er gedurende die tijd geen activiteiten zijn geweest in Easyflex. Dit is handig als iemand bijvoorbeeld vergeet om zijn/haar scherm te *locken* wanneer hij zijn/haar werkplek verlaat.

5. IP-filters/locaties afschermen

Naast toegangstijden kun je ook bepalend vanaf welke locaties, ofwel IP-adressen, er ingelogd mag worden. Ook deze instelling helpt mee om onrechtmatig gebruik van de applicatie te voorkomen. De IP-filters kun je als volgt vastleggen:

- Ga naar 'Beheer > IP filters'.
- Om een nieuw IP adres toe te voegen, klik je op de knop 'Nieuw'. In deze velden vul je het IP adres in. Vervolgens koppel je dit IP adres aan een werkmaatschappij of medewerker. Per IP filter kun je een omschrijving vastleggen.

6. Documenten verwijderen

Door de invoering van de AVG mag je minder gegevens én ook documenten bewaren. Zo schrijft een wijziging van de Waadi voor dat je sinds 1 januari 2018 binnen 4 weken een ID-bewijs moet verwijderen als de nieuwe kandidaat niet wordt geplaatst. En er zijn natuurlijk ook andere documenten die verwijderd moeten worden, de wettelijk verplichte bewaartermijnen hiervoor vind je in het bijgevoegde schema.

Als je documenten wilt kunnen verwijderen, moet je wel eerst zorgen dat je de juiste autorisatie hebt voor het verwijderen van de documenten. Dit doe je als volgt:

- Je kunt per documenttype een autorisatie vastleggen. Ga hiervoor naar 'Beheer > Document management > Document beheer'.
- Kies het tabblad 'Instellingen' en vink hier de autorisatie aan voor het verwijderen van documenten. Koppel hier dan een rol aan. Let op: Als dit vinkje uit staat, kunnen alle rollen documenten verwijderen.
- Je kunt ook een autorisatie vastleggen voor alléén ID bewijzen. Ga hiervoor naar Beheer > Bedrijfsinstellingen > Autorisatie flexwerkers. Onder "Autorisatie overige instellingen" kun je een vinkje zetten bij 'Verwijderen ID-bewijzen'. Koppel ook hier een rol aan. Let op: Als dit vinkje uitstaat, kunnen alle rollen de ID-bewijzen verwijderen.

Je kunt een (ingeplande) match draaien om te zien welke flexwerkers niet zijn geplaatst binnen vier weken en tegelijkertijd ook welke ID-bewijzen er verwijderd moeten worden. Dit doe je als volgt:

- Ga naar 'Frontoffice > Matching'. Kies hier voor 'Nieuw'.
- Kies dan voor selectie 'Flexwerker (handmatig)' en voer een kenmerk in (dit is de naam van de match, bijvoorbeeld: ID-bewijzen na 4 weken).
- Kies het selectieobject 'Status FW' en geef bij de 'Inschrijfdatum > Vanaf' een datum in het verleden in (minimaal 4 weken geleden).
- Vink bij 'Huidige status' alleen 'Ingeschreven' aan.
- Klik op 'Starten' om de match te starten. Als de match klaar is, kun je hem openen en naar 'Uitvoer samenstellen' gaan, dit staat rechts onderin.
- Vink de bovenste kwalificaties uit en vink (minimaal) het volgende aan: registratienummer, ingeschreven op, naam en identificatiebewijs. Sla dit vervolgens op.
- Tot slot kies je voor 'Batch actie' en bij selectie 'Export CSV'. Hiermee wordt een CSV-bestand gemaakt wat je in Excel kunt openen. De export vind je terug bij 'Backoffice > Exporteren en printen'. Naar aanleiding van deze lijst kun je vervolgens de ID-bewijzen die op deze lijst staan handmatig verwijderen.
- Je kunt er ook voor kiezen dit overzicht automatisch (regelmatig) aan te laten maken. Zorg er wel voor dat je ten minste één keer de match hebt aangemaakt. Ga voor het instellen van een ingeplande match naar 'Backoffice > Overzichten > overzicht Ingeplande matches'. Je kunt daar instellen dat dit overzicht bijvoorbeeld elke maand gedraaid wordt. Dit doe je onder het kopje 'Uitvoeren > Wanneer verwerken?'. Deze staat standaard op 'Direct', pas dit bijvoorbeeld aan naar 'Eind van elke maand'. Je kunt dit overzicht zelfs automatisch naar jezelf laten mailen, wanneer deze is aangemaakt. Dit doe je door op de drie puntjes te klikken achter 'Gereed melden aan'. Kies hier voor 'Nieuw' en vervolgens voor 'e-mail' onder type berichtgeving.

7. Autorisaties vastleggen

Je kunt voor elke gebruiker een autorisatie vastleggen in Easyflex. Dit helpt je om te sturen wie welke gegevens mag inzien. Je kunt dit bijvoorbeeld doen zodat loonbeslagen niet voor iedereen inzichtelijk zijn. Alleen degene die verantwoordelijk is voor de verwerking van het loonbeslag mag hierbij kunnen. Dit geldt ook voor bijvoorbeeld arbeidsongeschiktheid, ook ziekmeldingen kun je werken met autorisaties. Dit doe je als volgt:

- Ga naar 'Beheer > Medewerkers > Rollen'. Check welke rol een medewerker heeft of voeg er een toe.
- Ga naar 'Beheer > Programmarechten'. Hier kun je per rol aangeven welke tabbladen er zichtbaar zijn voor de gebruiker. De rechten zet je aan door deze aan te vinken.

8. Dataportabiliteit

De AVG introduceert per 25 mei een nieuw recht, namelijk het recht op dataportabiliteit. Simpel gezegd houdt dit in dat een flexwerker recht heeft op de overdraagbaarheid van gegevens. De flexwerker heeft dus het recht om zijn/haar persoonsgegevens, die zijn verstrekt aan een organisatie, zo snel mogelijk in een machine leesbare vorm te ontvangen. Om dit te bewerkstelligen in Easyflex, kun je een match uitdraaien. Deze match kun je vervolgens aanleveren aan de flexwerker als een export CSV bestand. Dit doe je als volgt:

- Ga naar 'Frontoffice > Matching' en kies 'Nieuw'.
- Kies selectie: 'Flexwerker (handmatig)'. Klik vervolgens op 'Toevoegen' onderin en voeg hier de desbetreffende flexwerker aan toe.
- Klik vervolgens rechts onderin op 'Uitvoer samenstellen' en selecteer hier de velden die je wil zien in de match. Dit kan bijvoorbeeld het volgende zijn: registratienummer, naam, identificatiebewijs e.d.
- Kies vervolgens voor 'Batch actie > Export CSV'. Je kunt de export nu vinden bij 'Backoffice > Exporteren en printen'. Deze kun je vervolgens als CSV-bestand aan je flexwerker aanleveren.