

PRIVACY STATEMENT | Dutch Mortgage Portfolio Management B.V. - employees

WHO ARE WE?

Dutch Mortgage Portfolio Management B.V. (hereafter referred to as DMPM) believes it is very important to protect the privacy of its employees. The personal data is processed in accordance with the General Data Protection Regulation (hereafter abbreviated to GDPR).

DMPM processes the personal data of its employees in its capacity as employer and also sometimes processes the personal data for its customers in its capacity as service provider. DMPM considers it important to provide you with clear information on how it uses your personal data within the organization.

This means that DMPM:

- **Clearly specifies the purposes of the processing** before the personal data is processed, including in the processing register.
- **Stores as little personal data as possible** and only processes that data which is needed for those purposes determined in advance.
- **Takes the necessary security measures** to protect your personal data. These obligations are also imposed on parties that process personal data on behalf of DMPM.
- **Respects the rights of our employees and customers**, such as the right to access, rectify, or erase the personal data that we process.
- **Processes as little special category personal data as possible** – this refers to data about a person's health, origin, or race, political opinions, sexual orientation, religious or philosophical beliefs, trade union membership, genetic data, and biometric data for the purpose of uniquely identifying a natural person.

The purpose of this privacy statement is to clearly set out how DMPM deals with your personal data.

WHOSE PERSONAL DATA DO WE PROCESS?

DMPM processes the personal data of various groups of people. This privacy statement focuses on employees working for DMPM.

WHY DO WE PROCESS PERSONAL DATA?

We are only permitted to process personal data where we have a legal basis to do so. We use your personal data for the following purposes:

- **Execution of the employment contract or termination of the employment contract**
In principle, this includes everything needed to ensure that you can start working for us. It also includes arranging entitlements to benefits when your employment is terminated. We do this in order to execute the employment contract and also because we are required to do so by law. It includes:
 - Managing your work activities and supervising your development.
 - Performing HR activities (such as staff administration, payroll administration, and sickness registration).
 - Providing medical and/or social care from the company if necessary.
 - Internal control and business operations.
 - Implementing the employment conditions.

- **Internal election of members for participation bodies**
When filling positions in participation bodies, such as the works council, we operate on the basis of a democratic model. Should you wish to take part in elections to become a member of a body, your personal data will be processed as we need these details to enable you to fulfil this role.
- **Performance of an accounting audit**
During an accounting audit, personal data is processed, for example to check the payroll records.
- **Configuring and managing company equipment**
To enable you to do your work, we provide you with a laptop and possibly also a telephone. These devices are installed with a Citrix environment. These applications are used to configure, locate, and manage the devices remotely. We have a legitimate interest in doing this. By using these applications, we maintain control of the devices that have access to company critical data and can guarantee the right protection.
- **Access to business mailbox**
We can grant ourselves access to your business mailbox. This may be necessary so that we can arrange matters if you unexpectedly become ill or if you leave the company. We will not read the emails in your business mailbox without informing you about this. In addition, we will ask for prior permission from you where possible. Should your business mailbox contain any personal emails, mark them as private and transfer them to a separate folder. We will not open these emails.
- **Logging**
We keep log files of our ICT systems. We use logging to find out what information you consult and when you do so. We have a legitimate interest in doing this. Logging enables us to reduce our security risks. We will not use the data to assess the performance of our employees.
- **Monitoring ICT and network traffic of employees**
We monitor the use of ICT and network traffic via company equipment and the company network. We have a legitimate business interest in doing this. Monitoring enables us to reduce security risks, detect crimes (such as illegal downloading), and resolve labour disputes. We will not use the data to assess your performance and will only monitor specific aspects if our systems discover risks.
- **Protecting our premises and company equipment**
We make use of camera surveillance to protect our premises and our company equipment. We have a legitimate interest in recording the footage and will only look at this footage if we have specific grounds for suspecting that a criminal offence has occurred. By using camera surveillance, we can help to prevent thefts and provide our employees with a certain level of protection. The camera footage will not be used to check how you do your work and only the persons directly involved will have access to the images.
- **Emergencies**
Should something happen to you during working hours, such as an accident or acute illness, then we will contact the person you specified for emergency situations. We do this because it is necessary to protect your vital interests.
- **Training and development**
Your manager can arrange with you that you take part in training or attend a course because of your job. To enable you to do so, we pass on your personal data to external trainers and record internally which training programmes or courses you participate in.

WITH WHOM DO WE SHARE YOUR PERSONAL DATA?

We will only share your personal data with other companies or institutes if this is legally permitted. This may be to comply with a legal obligation (collection of wage tax), for example, or to be able to execute the employment contract (pension provider).

In any case, we share this data with the following parties:

PARTY	PURPOSE	TYPE OF DATA
Pension provider/Insurance companies	So that the administrator can maintain pension accounts and so that you build up a pension.	Name and address details, salary details, and whether you are married, unmarried, or in a registered partnership.
Payroll administration company	So that you can access your financial details and information on your employment conditions.	
Accountant	During an accounting audit, personal data is processed, for example to check the payroll records.	
Dutch Tax Administration		The employer pays wage tax on behalf of its staff to the Dutch Tax Administration. The employer must register its employees for wage tax and national insurance contributions via the 'Statement of data for payroll taxes' form.
Employee Insurance Agency (UWV)	To pass on information so that matters such as employee insurance schemes, post-birth leave, and absenteeism can be arranged.	UWV has its own employer portal where employers can enter information and arrange matters, such as reporting employees sick and better, uploading rehabilitation reports, and requesting pregnancy leave etc.
IT service providers	To enable you to do your work, we provide you with a laptop and possibly also a telephone. These devices are installed with a Citrix environment. These applications are used to configure, locate, and manage the devices remotely. We have a legitimate interest in doing this. By using these applications, we maintain control of the devices that have access to	

	company critical data and can guarantee the right protection.	
--	---	--

In order to carry out the work and complete business administration tasks, your personal data may also be processed by the different entities within the Blauwtrust Groep. In this case, your personal data will only be shared if this is necessary to carry out these tasks and only with the employees authorized for this purpose.

We have entered into a processing agreement or a data exchange agreement with the parties with whom this is required by law, in which agreements are made regarding what may be done with your data and how it will be suitably protected. Some of the abovementioned parties have autonomous responsibility. They have their own basis for processing your data, such as the Dutch Tax Administration.

It may be possible that companies or institutes to whom we pass on your personal data are based outside the European Economic Area (EEA). We make sure that we only pass on your personal data – and also that of our customers, partners, or suppliers – to companies or institutes outside the EEA if all legal conditions have been met.

WHAT PERSONAL DATA DO WE PROCESS?

In the context of the employment contract, we process the following data:

- I. **Contact details** (such as name, address, place of residence, business and private email addresses, and business and private telephone numbers).
- II. **Identification details** (such as Citizen Service Number (BSN), ID number, date of birth, place of birth, gender, nationality, copy of ID).
- III. **Financial data** (such as: IBAN number(s), salary and other remunerations, bank account number).
- IV. **Sensitive/Special categories of personal data** (such as recording sickness absence without specifying the nature of the illness (Eligibility for Permanent Incapacity Benefit (Restrictions) Act), medical details where needed to properly execute the employment contract or to support your own health, copies of IDs, your citizen service number (BSN) and other identification numbers issued by the government, camera footage, and photos).
- V. **Interactions** (such as letters and emails that we send to you and receive from you, (protected) business emails that you send via your business email account).
- VI. **Work-related personal data:** (such as your position, employment contract and any amendments and appendices, signature, curricula vitae, certificate of good conduct (VOG), performance reports, payroll tax statement, presence and absence for payroll administration, registration of disciplinary action and complaints, registration of absence, information about work history and past education, attachment of earnings, vehicle registration number).
- VII. **Other relevant personal data** of importance (such as marital status and family composition, contact details for partner and/or child)

*We do not process any personal data revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, any genetic data, or any data concerning your sex life or sexual orientation.

WHAT IS THE BASIS FOR PROCESSING PERSONAL DATA?

It is only permitted to process personal data if there is a legal basis for doing so. We process the personal data of employees solely on the basis of one of the following reasons:

- **Execution of the employment contract or other contract** that we have entered into.
- A **legal obligation** to collect and store certain data, such as a copy of your ID and your citizen service number, as well as our statutory tax obligations such as preparing and keeping invoices and wage tax forms.
- We may sometimes process data because we have a **legitimate interest** in doing so. In that case, we have balanced our business interest against your right to privacy. One example is to ensure that our systems are properly protected.
- We may process personal data because we have been given **consent** to do so. We only do this if you actually have a free choice in the matter and there are no negative consequences if you do not give consent. You can always withdraw your consent again.
- In exceptional situations, we may need your details to protect your life. This is considered to be a **vital interest**. These are life-threatening situations, such as an acute medical emergency situation which causes you to become unconscious. This is only done in exceptional cases.

HOW LONG DO WE KEEP YOUR DATA?

We keep your personal data for as long as it is relevant for the employment relationship, for as long as we are required to do so by law, or until there is no longer a need to keep the data. This means the following:

- We keep your certificate of good conduct (VOG) and assessments for a maximum of 60 days after you leave the company.
- We keep your personnel file containing reports of your performance reviews and appraisal interviews for up to two years after you leave the company.
- We keep your name and address details, date of birth, and citizen service number, as well as the information for income tax and a scan of your ID for up to five years after the year in which you leave the company, in accordance with the Implementing Regulations to the Wages and Salaries Tax Act.
- We keep the payroll records for seven years after the year in which the wage was earned, in accordance with the retention obligation for tax records.
- We keep timekeeping records for no longer than legally required from us on the basis of tax and labour legislation.
- We keep email messages (both internal and external) that relate to business operations for seven years after the send date, in accordance with tax legislation.

At the end of the retention period, your personal data will be erased or anonymized. Anonymizing the personal data means that it is stripped of all possible identifying characteristics so that no one can see that the data is about you.

HOW DO WE PROTECT YOUR DATA?

We do our utmost to protect your personal data as much as possible. We take both technical and organizational measures to protect the personal data that we process. We do this in accordance with the applicable legal requirements and guidelines. In any case, we take the following measures:

- We invest in our systems, procedures, and people.
- We make sure that we work in a way that is appropriate for the sensitivity of your personal data.
- We adopt a strict password policy.
- Your personal data can only be accessed by a few authorized employees.
- We make use of Multifactor authentication.
- We make use of logging so that we can keep track of exactly who does what with your personal data.
- We train our people to treat your personal data securely.
- Our online services are protected.
- Personal data is stored and sent encrypted as much as possible.

WHAT RIGHTS DO YOU HAVE?

As the data subject, you have certain rights with regard to the processing of your personal data. You may exercise these rights in respect of your employer DMPM. You have the following rights:

- I. **Right of access:** You have the right to access your personal data and can generally obtain access to your personal data that we process within a month of submitting your request to us.
- II. **Right to rectification:** You can ask us to correct or complete any incorrect or incomplete details in your personal data.
- III. **Right to erasure:** You can ask us to remove your personal data in certain circumstances. In this case, we will take reasonable steps to inform other processors that process the personal data on our behalf that you have requested the removal of links to and copies of your personal data.
- IV. **Restriction of processing:** In certain circumstances, you can ask us to restrict the processing of personal data (either temporarily or permanently), e.g. if you contest the accuracy of personal data.
- V. **Right to data portability:** You can ask for the personal data you provided us with and which we store in a computerized manner to be given to you in a structured, commonly used, and machine-readable format so that, for instance, you can send it to a third party.
- VI. **Right to object:** You have the right to object to the processing of your personal data on the basis of a legitimate interest.
- VII. **Submitting a complaint:** You may submit a complaint regarding the processing of your personal data. First submit a complaint to DMPM's Privacy Officer or subsequently to the Data Protection Officer of the Blauwtrust Groep (DPO). If you do not agree with the way your request has been handled, you can then submit a complaint to the Dutch Data Protection Authority (Dutch DPA).

Exceptions may apply when exercising these rights, which means that we may not be able to provide a positive response to all requests, for example if DMPM is legally obliged to retain your personal data for a specific period.

Do you wish to exercise your rights, submit a complaint, or ask a question?

Send us a letter or email with your request to exercise your rights. In principle, we will meet your request within a month. However, this deadline may be extended to a maximum of three months if the request is complex or because there are many requests that need to be handled at the same time. If we need to extend this deadline, we will inform you of this in time.

If you still have questions or would like to exercise one of your rights, please send a letter or email to the Privacy Officer:

Email: privacy@dmpm.nl

DMPM
Attn: Privacy Officer DMPM
Postbus 306
3000 AH Rotterdam
(The Netherlands)

If you would like to submit a complaint about the way that DMPM handles your personal data or the way in which DMPM has dealt with your request to exercise your rights as data subject, please contact the Data Protection Officer of the Blauwtrust Groep.

Email: dpo@dmpm.nl

Dutch Mortgage Portfolio Management (DMPM)
Attn: Data Protection Officer DMPM
P.O.Box 306
3000 AH Rotterdam
(The Netherlands)

You may also submit a complaint to the Dutch Data Protection Authority (Dutch DPA) at any time. Use the form on the Dutch DPA [website](#) to do so. However, we do advise you to always submit a complaint to the Blauwtrust Groep first.

CHANGES TO OUR PRIVACY STATEMENT

If legislative changes occur or changes are made to our services and products, this may have consequences for the way in which we use your personal data. In that case, the privacy statement will be amended and we will inform you about this by sharing the new version with you. You can see from the version number and date at the bottom of the privacy statement whether changes have been made.

Version 1.0
May 2022

PRIVACY STATEMENT | Dutch Mortgage Portfolio Management B.V. - medewerkers

WIE ZIJN WE?

Dutch Mortgage Portfolio Management B.V. (hierna DMPM) vindt de privacy van haar werknemers zeer belangrijk. Het verwerken van persoonsgegevens vindt dan ook plaats overeenkomstig de vereisten uit de Algemene verordening gegevensbescherming (hierna: AVG).

DMPM verwerkt in haar rol van werkgever persoonsgegevens van jouw als medewerker en soms in de rol van dienstverlener als DMPM persoonsgegevens voor haar klanten verwerkt. DMPM vindt het belangrijk om je goed te informeren over het gebruik van je persoonsgegevens binnen de organisatie.

Dit betekent dat DMPM:

- **De doeleinden voor verwerking duidelijk vastlegt** voordat er persoonsgegevens worden verwerkt, onder andere in het verwerkingsregister.
- **Zo min mogelijk persoonsgegevens** opslaat en enkel de gegevens die nodig zijn voor de vooraf vastgestelde doeleinden verwerkt.
- **Benodigde beveiligingsmaatregelen treft** om je persoonsgegevens te beschermen. Deze verplichtingen worden ook opgelegd aan partijen die persoonsgegevens voor DMPM verwerken.
- **De rechten van onze werknemers en klanten respecteert**, zoals het recht op inzage, correctie of verwijdering van de bij ons verwerkte persoonsgegevens.
- **Zo min mogelijk bijzondere persoonsgegevens verwerkt**, dat zijn gegevens over iemands gezondheid, afkomst of ras, politieke gezindheid, seksuele voorkeur, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, en biometrische gegevens met het oog op de unieke identificatie van een persoon.

Via deze privacyverklaring wil DMPM je duidelijk maken hoe zij met jouw persoonsgegevens omgaat.

WIENS PERSOONSgegevens VERWERKEN WIJ?

DMPM verwerkt persoonsgegevens van verschillende groepen personen. Deze privacyverklaring ziet op medewerkers van DMPM.

WAARVOOR VERWERKEN WIJ PERSOONSgegevens?

Wij mogen persoonsgegevens alleen verwerken, wanneer wij daar een rechtmatige grondslag voor hebben. Wij gebruiken je persoonsgegevens voor de volgende doeleinden:

- **Uitvoering geven aan de arbeidsovereenkomst of beëindiging van de arbeidsovereenkomst**
In principe valt hier alles onder waardoor wij ervoor kunnen zorgen dat je bij ons aan de slag kunt. Ook valt hier bijvoorbeeld onder het regelen van aanspraken op uitkeringen wanneer je dienstverband wordt beëindigd. Wij doen dit om de arbeidsovereenkomst uit te kunnen voeren, maar ook omdat wij daartoe wettelijk verplicht zijn. Denk hierbij aan:
 - Leidinggeven aan je werkzaamheden en de begeleiding in je ontwikkeling.
 - Uitvoering van HR-activiteiten (zoals personeelsadministratie, salarisadministratie en ziekteregistratie).
 - Het bieden van bedrijf medische en/of maatschappelijke zorg indien nodig.
 - Interne controle en bedrijfsvoering.

- Uitvoering geven aan de arbeidsvoorwaarden.
- **Interne verkiezingen van leden voor medezeggenschapsorganen**
 Voor de invulling van functies van medezeggenschapsorganen zoals de ondernemingsraad hanteren wij een democratisch model. Mocht je mee willen doen aan verkiezingen van een orgaan, dan worden daarvoor jouw persoonsgegevens verwerkt, omdat we die nodig hebben om je deze functie te laten vervullen.
- **Het (laten) uitoefenen van een accountantscontrole**
 Bij een accountantscontrole worden persoonsgegevens verwerkt bijvoorbeeld om de salarisadministratie te controleren.
- **Het configureren en beheren van bedrijfsapparatuur**
 Om uw werkzaamheden te kunnen doen ontvangt je een laptop, en soms ook een telefoon van ons. Deze apparaten zijn uitgerust met een Citrix omgeving. Door middel van deze applicaties kunnen de apparaten op afstand geconfigureerd, gelokaliseerd en beheerd worden. Wij hebben hierbij een gerechtvaardigd belang. Door het gebruik van deze applicaties houden wij grip op de apparaten die toegang hebben tot bedrijf kritische gegevens en kunnen wij de juiste beveiliging garanderen.
- **Toegang zakelijke mailbox**
 Wij kunnen onszelf toegang geven tot jouw zakelijke mailbox. Dit kan bijvoorbeeld nodig zijn om zaken te kunnen regelen wanneer je onverwacht ziek bent geworden of wanneer je niet langer bij ons in dienst bent. We zullen de e-mails in jouw zakelijke mailbox niet lezen, zonder dat je hiervan op de hoogte bent gesteld. Daarnaast zullen we je, waar mogelijk, om voorafgaande toestemming vragen. Mochten er persoonlijke e-mails in jouw zakelijke mailbox zitten, markeer deze dan als privé en plaats ze in een apart mapje. Deze e-mails zullen we niet openen.
- **Logging**
 Wij houden logbestanden van onze ICT-systemen bij. Met logging kunnen we achterhalen welke informatie op welk tijdstip wordt geraadpleegd door je. Hier hebben we een gerechtvaardigd belang bij. Door logging kunnen we namelijk onze beveiligingsrisico's verkleinen. Wij zullen de gegevens niet gebruiken om het functioneren van medewerkers te beoordelen.
- **Het monitoren van ICT- en netwerkbeheer van werknemers**
 Wij monitoren het gebruik van ICT- en netwerkverkeer via bedrijfsapparatuur en het bedrijfsnetwerk. Wij hebben hiervoor een gerechtvaardigd bedrijfsbelang. Door te monitoren kunnen we beveiligingsrisico's verkleinen, misdrijven opsporen (zoals illegaal downloaden), en arbeidsconflicten oplossen. Wij zullen de gegevens niet gebruiken om jouw functioneren te beoordelen en zullen enkel gericht monitoren als onze systemen risico's ontdekken.
- **Het beveiligen van onze panden en bedrijfsmiddelen**
 Wij maken gebruik van cameratoezicht, ter bescherming van ons pand en onze bedrijfsmiddelen. Wij hebben een gerechtvaardigd belang bij het opnemen van de camerabeelden en zullen deze beelden alleen raadplegen in geval van een concreet vermoeden van een strafbaar feit. Door gebruik te maken van cameratoezicht kunnen wij diefstal tegengaan en onze werknemers een bepaald beschermingsniveau bieden. De camerabeelden zullen niet worden gebruikt om te controleren hoe jij je werkzaamheden uitvoert en alleen de direct betrokken personen hebben toegang tot de beelden.
- **Calamiteiten**
 Mocht er iets met je gebeuren onder werktijd, bijvoorbeeld een ongeval of acute ziekte, dan nemen wij contact op met de persoon die je hebt opgegeven voor noodsituaties. Wij doen dit omdat het noodzakelijk is om jouw vitale belangen te beschermen.
- **Training en ontwikkeling**

Jouw leidinggevende kan met je afspreken dat je trainingen volgt of bij een cursus aanwezig bent, uit hoofde van jouw functie. Om je hiertoe gelegenheid te geven, geven we jouw persoonsgegevens door aan externe opleiders en registreren we intern welke opleidingen of cursussen je hebt bijgewoond.

MET WIE DELEN WIJ JOUW PERSOONSGEGEVENS?

Wij delen jouw persoonsgegevens alleen met andere bedrijven of instellingen, wanneer dat wettelijk is toegestaan. Bijvoorbeeld voor het voldoen aan een wettelijke plicht (loonbelasting doorvoeren) of om de arbeidsovereenkomst te kunnen uitvoeren (pensioenverstrekker).

De partijen waarmee wij in ieder geval gegevens delen zijn:

PARTIJ	DOEL	SOORT GEGEVENS
Pensioenverstrekker-Verzekeringsbedrijven	Zodat de uitvoerder de pensioenadministratie kan voeren en voor jou de pensioenopbouw plaats vindt.	NAW gegevens, Salarisgegevens, gehuwd, ongehuwd dan wel geregistreerd partnerschap.
Salarisadministratiekantoor	Zodat je (online) inzag hebt in je financiële en arbeidsvoorwaardelijke gegevens.	
Accountant	Bij een accountantscontrole worden persoonsgegevens verwerkt bijvoorbeeld om de salarisadministratie te controleren.	
Belastingdienst		Werkgever betaalt de loonbelasting van personeel aan de Belastingdienst. Werkgever moet de medewerker aanmelden voor de loonheffingen via formulier 'Opgaaf gegevens voor de loonheffingen'.
UWV	Doorgeven informatie voor het regelen van zaken zoals werknemersverzekeringen, geboorteverlof en verzuim.	UWV heeft een eigen werkgeversportaal waar werkgevers zaken in moeten voeren en regelen zoals medewerkers ziek en betermelden, Re-integratieverslagen uploaden en aanvragen zwangerschapsverlof etc.
IT-dienstverlener(s)	Om uw werkzaamheden te kunnen doen ontvangt je een laptop, en soms ook een telefoon van ons. Deze apparaten zijn uitgerust met een Citrix omgeving. Door middel van deze applicaties kunnen de apparaten	

	op afstand geconfigureerd, gelokaliseerd en beheerd worden. Wij hebben hierbij een gerechtvaardigd belang. Door het gebruik van deze applicaties houden wij grip op de apparaten die toegang hebben tot bedrijf kritische gegevens en kunnen wij de juiste beveiliging garanderen.	
--	--	--

Voor het uitvoeren van de werkzaamheden en voeren van de bedrijfsadministratie worden jouw persoonsgegevens mogelijk ook verwerkt door de verschillende entiteiten binnen de Blauwtrust Groep. Hierbij worden de persoonsgegevens alleen gedeeld indien dit noodzakelijk is voor de uitvoering van deze werkzaamheden en enkel met de hiertoe bevoegde medewerkers.

Met de partijen waar dit wettelijk gezien nodig is, hebben wij een verwerkersovereenkomst of een gegevensuitwisselingsovereenkomst gesloten waarin afspraken zijn gemaakt over wat er met jouw gegevens gedaan mag worden en op welke wijze deze adequaat beveiligd zijn. Sommige van bovengenoemde partijen zijn zelfstandig verantwoordelijk. Zij hebben een eigen grondslag om je gegevens te verwerken, zoals de belastingdienst.

Het kan voorkomen dat de bedrijven of instellingen waaraan we jouw persoonsgegevens doorgeven buiten de Europese Economische Ruimte (EER) gevestigd zijn. Wij zorgen ervoor dat wij je persoonsgegevens, en ook die van onze klanten, partners of leveranciers, alleen doorgeven aan bedrijven of instellingen buiten de EER als voldaan is aan alle wettelijke voorwaarden.

WELKE PERSOONSgegevens VERWERKEN WIJ?

In het kader van de arbeidsovereenkomst, verwerken wij de volgende gegevens:

- VIII. **Contactgegevens** (zoals: naam, adres, woonplaats, (zakelijke en persoonlijke) e-mailadres, (zakelijke en persoonlijke) telefoonnummer(s)).
- IX. **Identificatiegegevens** (zoals: Burger Service Nummer (BSN), ID-nummer, geboortedatum, geboorteplaats, geslacht, nationaliteit, kopie van identiteitsbewijzen).
- X. **Financiële gegevens** (zoals: IBAN-nummer(s), salaris en andere vergoedingen, bankrekeningnummer).
- XI. **Gevoelige/Bijzondere categorieën van persoonsgegevens** (zoals: vastlegging van afwezigheid wegens ziekte zonder de aard van de ziekte te noemen (Wet verbetering Poortwachter) medische gegevens voor zover dat noodzakelijk is voor een goede uitvoering van de arbeidsovereenkomst of ten behoeve van jouw eigen gezondheid, kopieën van identiteitsbewijzen, BSN en andere identificatienummers van de overheid, camerabeelden, foto's).
- XII. **Contactmomenten** (zoals: brieven en e-mails die wij sturen en van je ontvangen, (afgeschermd) zakelijke e-mails die je verstuurt via jouw zakelijke mailaccount).
- XIII. **Werk gerelateerde persoonsgegevens:** (zoals: functie, de arbeidsovereenkomst en eventuele aanpassingen en bijlagen, handtekening, curricula vitae, Verklaring Omtrent het Gedrag (VOG) functioneringsverslagen, loonbelastingverklaring, aan- en afwezigheid salarisadministratie, disciplinaire- en klachtenregistraties, afwezigheidsregistratie, informatie over arbeidsverleden en opleidingsverleden, loonbeslag, kenteken)
- XIV. **Overige relevante persoonsgegevens** die van belang zijn (zoals: burgerlijke staat en gezinssamenstelling, contactgegevens partner en/of kind)

*Wij verwerken geen persoonsgegevens die betrekking hebben op uw ras of etnische afstamming, politieke opvattingen, religieuze of filosofische overtuigingen, lidmaatschap van een vakbond, genetische gegevens of gegevens met betrekking tot uw seksleven of seksuele oriëntatie.

WAT IS DE GRONDSLAG VOOR HET VERWERKEN VAN JOUW PERSOONSgegevens?

Het verwerken van persoonsgegevens is alleen toegestaan als hier een juridische basis (grondslag) voor is. Wij verwerken persoonsgegevens van werknemers enkel op basis van een van de volgende grondslagen:

- De **uitvoering van de (arbeids-)overeenkomst** die we hebben gesloten.
- Een **wettelijke verplichting** om bepaalde gegevens te verzamelen en te bewaren, zoals een kopie van jouw identiteitsbewijs en je BSN, maar denk hierbij ook aan onze fiscale wettelijke verplichtingen zoals het opstellen en bewaren van facturen en loonbelastingformulieren.
- Het komt voor dat wij gegevens verwerken omdat wij daar een **gerechtvaardigd belang** bij hebben. In dat geval hebben we een afweging gemaakt tussen ons bedrijfsbelang en jouw recht op privacy. Bijvoorbeeld om te zorgen voor goed beveiligde systemen.
- Wij kunnen persoonsgegevens verwerken omdat we daarvoor **toestemming** hebben verkregen. Dit doen wij alleen als je ook echt een vrije keuze hebt en er geen negatieve gevolgen zijn als je geen toestemming geeft. Toestemming kan ook altijd weer worden ingetrokken.
- In uitzonderingssituaties hebben we jouw gegevens nodig om je leven te beschermen. Er is dan een zogenaamd **vitaal belang**. Het gaat dan om levensbedreigende (nood)situaties. Denk bijvoorbeeld aan een acute medische noodsituatie waardoor je bewusteloos raakt. Dit komt enkel voor in uitzonderlijke gevallen.

HOE LANG BEWAREN WIJ JOUW GEGEVENS?

Wij bewaren jouw persoonsgegevens zo lang deze relevant zijn voor de arbeidsrelatie, zolang de wet ons dat verplicht of totdat er geen noodzaak meer bestaat om de gegevens te bewaren. Dit betekent het volgende:

- Wij bewaren jouw Verklaring Omtrent het Gedrag (VOG) en assessments tot maximaal 60 dagen na uitdiensttreding.
- Wij bewaren jouw personeelsdossier met daarin onder andere verslagen van jouw functionerings- en beoordelingsgesprekken tot maximaal 2 jaar na uitdiensttreding.
- Wij bewaren jouw NAW-gegevens, geboortedatum en BSN, alsmede de gegevens voor de inkomstenbelasting en een scan van je ID-bewijs tot 5 jaar na het jaar waarin je uit dienst treedt, conform de Uitvoeringsregeling loonbelasting.
- Wij bewaren de salarisadministratie 7 jaar na het jaar dat het loon is verworven, conform de fiscale bewaarplicht.
- Wij bewaren de urenregistratie niet langer dan wettelijk van ons wordt vereist op grond van belasting- en arbeidswetgeving.
- Wij bewaren e-mailberichten (zowel intern als extern) die betrekking hebben op de bedrijfsvoering 7 jaar na de verzenddatum, conform de belastingwetgeving.

Na afloop van de bewaartermijn worden uw persoonsgegevens verwijderd of geanonimiseerd. Anonimiseren houdt in dat persoonsgegevens worden ontdaan van alle mogelijk identificerende kenmerken, zodat niemand nog kan zien dat het over jou gaat.

HOE BEVEILIGEN WIJ JOUW GEGEVENS?

Wij doen ons uiterste best om jouw persoonsgegevens zoveel mogelijk te beschermen. Wij nemen zowel technische als organisatorische maatregelen om de persoonsgegevens die wij verwerken, te beveiligen. Wij doen dit volgens de daarvoor geldende wettelijke eisen en richtlijnen. We nemen in ieder geval de volgende maatregelen:

- Wij investeren in onze systemen, procedures en mensen.
- Wij zorgen ervoor dat onze manier van werken past bij de gevoeligheid van jouw persoonsgegevens.
- Wij hanteren een strikt wachtwoordbeleid.
- Jouw persoonsgegevens zijn slechts toegankelijk voor enkele bevoegde medewerkers.
- Wij maken gebruik van Multi factor authenticatie.
- Wij maken gebruik van logging waardoor wij precies bijhouden wie wat met jouw persoonsgegevens doet.
- Wij trainen onze mensen om veilig om te gaan met jouw persoonsgegevens.
- Onze onlinediensten worden beveiligd.
- Persoonsgegevens worden zoveel mogelijk versleuteld opgeslagen en verstuurd.

WELKE RECHTEN HEB JE?

Als betrokkene heb je bepaalde rechten ten aanzien van de verwerking van je persoonsgegevens. Deze rechten kun je uitoefenen tegenover DMPM, jouw werkgever. Je hebt de volgende rechten:

- VIII. **Inzage:** Je hebt het recht op inzage in jouw persoonsgegevens en kunt over het algemeen binnen één maand na je verzoek aan ons inzage krijgen in de persoonsgegevens die wij van je verwerken.
- IX. **Rectificatie:** Je kunt aan ons vragen om onjuistheden in je persoonsgegevens te corrigeren of aan te vullen.
- X. **Verwijderen:** Je kunt ons vragen om persoonsgegevens onder bepaalde omstandigheden te verwijderen. Wij zullen in dit geval redelijke stappen nemen om andere verwerkers die namens ons de persoonsgegevens verwerken op de hoogte stellen dat je hebt verzocht om verwijdering van koppelingen naar en kopieën van jouw persoonsgegevens.
- XI. **Beperken van verwerking:** Je kunt ons onder bepaalde omstandigheden verzoeken om de verwerking van persoonsgegevens (al dan niet tijdelijk) te beperken, bijvoorbeeld als de juistheid van persoonsgegevens door je wordt betwist.
- XII. **Overdraagbaarheid:** Je kunt ons vragen om de persoonsgegevens die je aan ons hebt verstrekt en die wij geautomatiseerd opslaan, in een gestructureerde, gangbare en machine leesbare vorm van ons te verkrijgen, bijvoorbeeld om deze vervolgens te verzenden naar een derde partij.
- XIII. **Bezwaar:** Je hebt het recht om bezwaar te maken tegen een verwerking van je persoonsgegevens op basis van gerechtvaardigd belang.
- XIV. **Klacht indienen:** Je kunt een klacht over de verwerking van je persoonsgegevens indienen. Eerst dien je een klacht in bij de Privacy Officer van DMPM of vervolgens de Functionaris Gegevensbescherming Blauwtrust Groep (FG). Indien je het niet eens bent met de afhandeling van je verzoek, kun je daarna ook een klacht indienen bij de Autoriteit Persoonsgegevens (AP).

Bij de uitoefening van deze rechten kunnen uitzonderingen van toepassing zijn, wat betekent dat wij niet alle verzoeken positief kunnen beantwoorden, bijvoorbeeld als DMPM wettelijk verplicht is om jouw persoonsgegevens voor een bepaalde periode te bewaren.

Wil je jouw rechten uitoefenen, een klacht indienen of een vraag stellen?

Stuur ons een brief of e-mail met je verzoek om je rechten uit te oefenen. Wij zullen in principe binnen een maand aan je verzoek voldoen. Deze termijn kan echter worden verlengd naar maximaal 3 maanden, omdat het een complex verzoek is of, omdat er veel verzoeken tegelijkertijd moeten worden behandeld. Als wij deze termijn verlengen, zullen wij je daarvan tijdig op de hoogte stellen.

Als je nog vragen hebt of een van jouw rechten wilt uitoefenen, neem dan contact op met de Privacy Officer via post of e-mail:

E-mail: privacy@dmpm.nl

DMPM
T.a.v. Privacy Officer DMPM
Postbus 306
3000 AH Rotterdam
(Nederland)

Als je een klacht wilt indienen over de manier waarop DMPM omgaat met jouw persoonsgegevens of de manier waarop DMPM jouw verzoek met betrekking tot het uitoefenen van je rechten van betrokkene heeft afgehandeld, neem dan contact op met de Functionaris Gegevensbescherming van Blauwtrust Groep.

E-mail: dpo@dmpm.nl

DMPM
T.a.v. Functionaris Gegevensbescherming DMPM
Postbus 306
3000 AH Rotterdam
(Nederland)

Je kan ook te allen tijde een klacht indienen bij de Autoriteit Persoonsgegevens (AP). Dit kan via het formulier op de [website](#) van de AP. We raden je wel aan om een klacht altijd eerst bij Blauwtrust Groep zelf in te dienen.

WIJZIGING VAN DE PRIVACYVERKLARING

Als er wetswijzigingen plaatsvinden of wijzigingen optreden in onze diensten en producten, kunnen die gevolgen hebben voor de manier waarop wij jouw persoonsgegevens gebruiken. In dat geval wordt de privacyverklaring aangepast en informeren wij je daarover door de nieuwe versie met je te delen. Dat er wijzigingen zijn toegevoegd kun je herkennen aan het versienummer en de datum onder deze privacyverklaring.

Versie 1.0
Mei 2022