PRIVACYBELEID VOOR MEDEWERKERS

INTRODUCTIE

Beste medewerker, Telenet group is verantwoordelijk voor de verzameling en het gebruik van uw persoonsgegevens en we beschermen deze als een goede huisvader. Hoe we omgaan met privacy maakt deel uit van de verantwoordelijkheid die we hebben naar onze medewerkers. We willen duidelijk zijn over hoe belangrijk de privacy van onze medewerkers is en hoe deze wordt beschermd. Telenet group ziet toe op de naleving van alle toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG).

Dit privacybeleid informeert u over de verwerking van uw persoonsgegevens, welke persoonsgegevens over u worden verzameld, welke soorten verwerkingsactiviteiten worden uitgevoerd, met wie we uw gegevens delen, hoe we deze beschermen en welke privacyrechten u heeft.

I. Wie zijn wij?

Wij zijn Telenet group (met maatschappelijke zetel te Liersesteenweg 4, 2800 Mechelen). Dit privacybeleid is van toepassing op werknemers (en zie verder beneden) van de volgende entiteiten van de Telenet group groep:

- Telenet Retail BV
- Telenet Group NV
- Telenet BV

II. Wie wordt beschermd door dit privacybeleid?

Dit privacybeleid is van toepassing op al onze werknemers, d.w.z. alle werknemers van Telenet group en alle andere personen die in dienst zijn van Telenet group, met inbegrip van degenen die door een derde tijdelijk ter beschikking worden gesteld van Telenet group zonder dat zij met Telenet group verbonden zijn door een arbeidsovereenkomst of een nominale dienstverleningsovereenkomst. Voor de toepassing van dit privacybeleid omvat de term "werknemer" onze huidige en voormalige werknemers en iedereen die voor Telenet group werkt, met inbegrip van:

- Onafhankelijke dienstverleners;
- Personeel van onze leveranciers;
- Consultants;
- Uitzendkrachten;
- Stagiaires;

- Jobstudenten;
- Vrijwilligers.

Dit voor zover Telenet group persoonlijke data van deze personen verwerkt.

Er is een specifiek beleid voor sollicitanten dat u kunt raadplegen wanneer u een openstaande vacature opent op onze vacaturewebsite.

III. Welke persoonsgegevens verwerkt Telenet group en waarom?

WELKE GEGEVENS VERWERKEN WIJ?

Dit beleid is van toepassing op alle persoonsgegevens die worden verzameld, verwerkt en opgeslagen in het kader van uw arbeidsrelatie. Persoonsgegevens zijn gegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon. Het is dus alle informatie die een natuurlijke persoon direct of indirect identificeert, zoals een naam, personeelsnummer, telefoonnummer, adres, geboortedatum, maar ook een IP-adres, een foto, een vingerafdruk, enz. Wij kunnen verschillende categorieën van persoonsgegevens met betrekking tot onze werknemers verwerken, steeds in overeenstemming met de voorwaarden van de toepasselijke specifieke wettelijke bepalingen of CAO's. Het overzicht van de gegevens die wij verzamelen vindt u in de onderstaande tabel.

Identificatiegegevens	Gegevens die u kunnen identificeren zoals uw naam en voornaam, adres, e-mailadres, telefoonnummer, identiteitskaartnummer, geboortedatum, geboorteplaats, rijksregisternummer, nummerplaat, personeelsnummer enz.
Foto's en video's	Afbeeldingen van u of video's, bijvoorbeeld wanneer u deelneemt aan een personeelsevenement, beelden van bewakingscamera's, enz.
Communicatiegegevens	Audio-opnames (bijv. in het contactcenter), transcripties en samenvattingen van de gesprekken, chats met klanten, enz.
Familiale gegevens	Burgerlijke staat, gezinssamenstelling, naam van de echtgeno(o)t(e) of partner, aantal kinderen, naam en contactgegevens van de personen met wie contact moet worden opgenomen in geval van nood, enz.
Professionele details	Overzicht van je loopbaan, CV, referenties, sollicitatiebrief, training & development, ontslagbrief etc.
Contractgegevens	Arbeidsovereenkomst, loonstroken, belastingdocumenten, informatie enz.
Financiële gegevens	Bankrekeningnummer, salaris, bonussen, andere voordelen toegekend door Telenet group, betalingen door Telenet group, informatie over maaltijdcheques, pensioenplan, gegevens met betrekking tot uw pensioen, onkostennota's, enz.

Mobiliteitsgegevens	Informatie met betrekking tot bedrijfswagens, tankkaart, andere mobiliteitsplannen, enz.
Registratie en monitoring van gegevens	Het loggen van gegevens met betrekking tot uw gebruik van de Telenet group-applicaties en -apparaten, login en wachtwoorden om toegang te krijgen tot Telenet group-applicaties, enz.
Gegevens over samenwerking	Gegevens over je online samenwerking en communicatie op Telenet group-platformen (e-mails in Outlook, posts op het intranet, notulen van vergaderingen, opnames van vergaderingen, chats in Teams, enz.)
Gegevens met betrekking tot uw aanwezigheid in Telenet group-gebouwen en met betrekking tot thuiswerk	Gebruik van de toegangsbadge, registratie van de dagen van aanwezigheid op kantoor of van thuiswerk in de speciale tools, verbindingen met thuiswerkservers, registratie van de toegang tot de technische gebouwen zoals de kopstations, serverruimtes, enz.
Prompts	Prompts gebruikt in AI-tools van Telenet group
Gezondheidsgerelateerde gegevens	Gezondheidsgerelateerde gegevens, om onze verplichtingen inzake de arbeidswetgeving en de sociale zekerheid na te komen, zoals gezondheidsmonitoring op het werk, gezondheidsbeoordelingen, arbeidsongevallen, medische attesten met betrekking tot arbeidsongeschiktheid, gegevens met betrekking tot zwangerschap en moederschap, geboorte, adoptie- of pleegverlof, enz.
Prestatiegegevens	Tuchtdossiers, resultaten van functioneringsgesprekken, assessments, etc.
Mandaten	Wettelijke mandaten (functies in andere organisaties)
Uittreksel strafregister voor veiligheidscontrole	Voor specifieke functies zijn we wettelijk verplicht om onze werknemers te screenen en uittreksels uit het strafregister te verzamelen
Gedragsgegevens (cookies)	Gegevens verzameld via cookies die op de interne HR-intranetpagina's worden geplaatst (om te analyseren hoe de bezoekers van de pagina navigeren, om te tellen hoeveel bezoekers de pagina's raadplegen, enz.)

Waarom verwerken wij deze persoonsgegevens?

De onderstaande tabel geeft een overzicht van de doeleinden en rechtsgronden van de verwerking van uw persoonsgegevens:

Doeleinden	Beschrijving	Rechtsgrondslag
Personeelsadministratie en -beheer	Dit doel heeft betrekking op alle activiteiten met betrekking tot de administratie en het beheer van werknemers, waaronder: Loonadministratie, bonusberekening; Beheer van (collectieve) verzekeringen, pensioenen;	**Contractuele verplichting**, om de goede uitvoering van uw arbeidsovereenkomst te verzekeren, zoals de uitbetaling van uw loon of de terugbetaling van uw beroepskosten **Wettelijke** verplichting, om te voldoen aan de wettelijke vereisten, zoals de verplichting om gegevens

	Werkplanning (plannen en bewaken van taken, werkdruk en prestaties); Urenregistratie en vakantieplanning; Beheer van uw persoonlijk personeelsdossier; Loopbaanontwikkeling, selectie van opleidingen en studiepaden; Mobiliteitsmanagement.	met betrekking tot arbeidsovereenkomsten elektronisch door te geven aan administratieve organen voor de sociale en fiscale wetgeving **Gerechtvaardigd belang,** om een goed personeelsbeheer en de ontwikkeling, monitoring en het beheer van werknemers te waarborgen
Gezondheid en veiligheid van werknemers	Activiteiten met betrekking tot de veiligheid, gezondheid en het welzijn van mensen op het werk, waaronder: Beheer van afwezigheid; Beheer van incidenten; Berichtgeving.	**Wettelijke verplichting**, de verwerking is noodzakelijk volgens een wettelijke verplichting **Gerechtvaardigd belang**, de verwerking is voorzien in het arbeidsrecht, het sociale zekerheidsrecht of een collectieve overeenkomst
Veiligheidscontrole	Opvragen van het uittreksel uit het strafregister voor de functies waar een veiligheidscontrole dient te gebeuren. Deze opvraging gebeurt door een daartoe aangeduid team bij Security en wordt afzonderlijk bewaard op een afgeschermde folder	**Wettelijk verplichting,** voor specifieke functies zijn we wettelijk verplicht om deze veiligheidscontrole uit te voeren (bv. de wet Jambon betreffende de bewakingsagenten)
IT-beveiliging, fraude en softwarebeheer	Activiteiten met betrekking tot het monitoren van het gebruik van de IT-infrastructuur die ter beschikking wordt gesteld aan de medewerkers (telefoon, e-mails, internet, applicaties), fraudepreventie, fraudedetectie en licentiebeheer.	Gerechtvaardigd belang
Fysieke beveiliging	Activiteiten om de veiligheid van goederen en personen in en rond onze kantoren en gebouwen te waarborgen.	Contractuele verplichting Gerechtvaardigd belang
Organisatie van personeelsevenementen	Activiteiten met betrekking tot de organisatie van evenementen, waaronder registratie voor deelname, foto's, gemaakte video's	**Toestemming**: in de relatie werkgever – werknemer vormt toestemming geen wettelijke basis omdat de werknemer zich in een ondergeschikte relatie met zijn/haar werkgever bevindt en niet in staat is om een vrije toestemming te geven. Niettemin is Telenet group van mening dat het zich in uitzonderlijke omstandigheden op toestemming kan beroepen wanneer de toestemming vrijelijk kan worden gegeven omdat werknemers geen enkele nadelige gevolgen zullen ondervinden,

		ongeacht of ze al dan niet toestemming geven
Analytics en strategische personeelsplanning	Interne rapportage, analyse en statistische inzichten, activiteiten met betrekking tot enquêtes zoals ZOOM	Gerechtvaardigd belang
Kwaliteitscontrole van de dienstverlening	Bewaking en analyse interacties tussen klanten en het klantenserviceteam om de klantervaring en de kwaliteit van de geleverde service te bewaken en te verbeteren. Inclusief gespreksopnames voor kwaliteitsmanagement	Gerechtvaardigd belang
AI-training	Activiteiten met betrekking tot de training van AI-tools en het gebruik van persoonsgegevens om grote taalmodellen te trainen	Gerechtvaardigd belang
Kennismanagement en inzichten	Analyseren van het gebruik van geleverde applicaties, inclusief prompt monitoring	Gerechtvaardigd belang
Analyses website bezoek	Cookies geplaatst bij website bezoek	Indien deze cookies geen functioneel doel hebben maar bedoeld zijn om analyses te doen (zoals het aantal bezoekers te tellen), is **toestemming** de legale grond

BIJZONDERE GEVALLEN

1. TOEZICHT OP HET GEBRUIK VAN IT-TOOLS

Telenet group kan gegevens over u verzamelen in het kader van het monitoren van het gebruik van uw pc en de toegang tot het internet, de IT-systemen, het netwerk en de applicaties. Deze controle wordt uitgevoerd om de veiligheid, de werking van de IT-tools die ter beschikking worden gesteld aan de werknemers en de goede uitvoering van verplichtingen (vastgelegd in de arbeidsovereenkomst of andere contracten) te waarborgen. In bepaalde specifieke gevallen, ook om ervoor te zorgen dat de werknemers de ethische waarden van Telenet group respecteren en om de vertrouwelijkheid van de strategische, financiële of commerciële belangen van Telenet group te beschermen. De gegevens die worden verzameld voor controledoeleinden zijn vertrouwelijk. In geval van een ernstig vermoeden van ongeoorloofd gebruik of inbreuk, kunnen deze gegevens worden geanalyseerd volgens bepaalde zeer nauwkeurige regels.

2. TOEGANG TOT DE ZAKELIJKE E-MAILS VAN DE WERKNEMER EN GEGEVENS DIE OP HARDE SCHIJVEN ZIJN OPGESLAGEN IN GEVAL VAN LANGDURIGE AFWEZIGHEID, VERMOEDEN VAN FRAUDE, SCHENDING VAN HET BEVEILIGINGSBELEID, ONTSLAG OF VERTREK

Telenet group kan, met strikte inachtneming van de beginselen van legitimiteit, transparantie, noodzakelijkheid en proportionaliteit, toegang krijgen tot de professionele e-mails van de werknemer in geval van langdurige afwezigheid, onderzoek naar fraude, vermoeden van inbreuk op het beveiligingsbeleid, maar ook na ontslag of vertrek van de werknemer. Deze toegang zal enkel gebeuren in gevallen waarin het noodzakelijk is om de continuïteit van een dienst te verzekeren, om de belangen van Telenet group te beschermen en zal steeds voorzien in een vier-ogen-principe (betrokkenheid Security).

Elke medewerker heeft de mogelijkheid om een 'Privé' Outlook-map aan te maken om zijn of haar privé-e-mailcommunicatie op te slaan. In geval van toegang tot de e-mail inbox tijdens een langdurige afwezigheid of onderzoek, is elke toegang tot deze map door een andere persoon dan de betreffende medewerker niet toegestaan.

3. INZICHTEN EN ANALYSES

Uw persoonsgegevens kunnen worden gebruikt in interne analyses die Telenet group helpen bij het nemen van weloverwogen beslissingen, het bepalen van een goede HR-strategie en het creëren van inzichtelijke rapporteringen. Toegang tot gegevens op werknemersniveau is beperkt tot het aangestelde People Analytics-team en wordt alleen op geaggregeerde basis buiten dit team gedeeld.

Dit omvat bijvoorbeeld

- Analyses met betrekking tot telewerken, ter ondersteuning van een beter beheer van middelen in hybride werkscenario's: gegevens die uit het toegangsbadgesysteem worden opgehaald, worden verwerkt om de aanwezigheid op kantoor te berekenen en worden op teamniveau gerapporteerd. Teamresultaten worden gepresenteerd ongeacht de teamgrootte. Omdat dit objectief en observeerbaar gedrag is, passen we niet de minimale aggregatie van 5 medewerkers toe zoals we doen voor gevoelige en subjectieve gegevens zoals ZOOM-resultaten.

- Analytics met betrekking tot het gebruik van de Microsoft-applicaties voor een optimale licentieverdeling: statistische gegevens die uit het Microsoft-platform worden gehaald, geven (kwantitatief) inzicht in uw gebruik van de Microsoft-applicaties (gebruik van Teams, Outlook, ...). De statistieken worden niet gerapporteerd, maar worden door Digital Workplace gebruikt om de distributie van softwarelicenties te prioritiseren en te optimaliseren, bijvoorbeeld voor Microsoft Copilot-licenties.

- Analyse met betrekking tot Viva Insights: geaggregeerde rapporten over de Viva Insights-statistieken, verrijkt met de ZOOM-resultaten, bieden zinvolle inzichten in cultuur, vergaderkosten, balans tussen werk en privéleven, enz.

- Analyses met betrekking tot hardwaremonitoring en activabeheer: statistische gegevens over uw pc (bijv. statistieken over pc-crashes, gebruik van de opslagcapaciteit, geïnstalleerde apps) worden verzameld en samengevoegd voor inzichten in activabeheer en toewijzing van toestellen.

- Expedition T datagestuurde individuele aanbevelingen: op basis van de kwalificaties die je in Expedition T hebt ingevoerd, worden je interne vacatures en leeractiviteiten aanbevolen in Expedition T.

- Analyse voor HR-KPI's: gegevens afkomstig uit de ZOOM-enquêtes, uit het toegangsbadgesysteem en uit HR-applicaties (met betrekking tot salarisadministratie en beloning, samenwerking, prestatiebeheer, carrièrepad en leren) worden gecombineerd voor inzichtelijke correlaties en gerapporteerd, op geaggregeerde basis.

4. GEGEVENS VOOR AI-TRAINING EN HET GEBRUIK VAN AI-TOOLS VAN TELENET GROUP

Telenet group biedt meerdere AI-ondersteunde tools aan. Er zijn situaties mogelijk waarbij AI tools uw persoonlijke data zullen verwerken. Er wordt steeds contractueel vastgelegd dat de AI provider de Telenet group-data (en dus ook uw persoonlijke gegevens) niet mag hergebruiken bv. om zijn AI model verder te trainen. Een voorbeeld van een AI tool dat persoonlijke data zal verwerken is de Agent Assist. Agent Assist is een tool die de gesprekken met klanten transcribeert en een samenvatting na het gesprek voorstelt. De tool verbetert ook de prestaties van agenten door realtime ondersteuning te bieden tijdens gesprekken, inclusief onmiddellijke feedback, live luisteren naar vragen en fluisteren van antwoorden aan agenten. Deze AI tool zal meeluisteren met het gesprek en het gesprek omzetten naar een transcriptie. Ook zal een instructie (een prompt) aan een Gen-AI taalmodel worden gegeven om de transcriptie samen te vatten. Na oplevering van deze samenvatting wordt de transcriptie en de instructie verwijderd uit het Gen-AI taalmodel. De leverancier van het Gen-AI taalmodel hergebruikt de transcriptie niet. Net zoals de opnames bij Telenet group gedurende één maand worden bewaard, worden ook de transcripties gedurende één maand bewaard.

Indien Telenet group zelf een gen-AI model wil trainen, dan gebeurt dit in eerste instantie steeds met niet-persoonsgebonden data of synthetische data. Afhankelijk van de situatie kan het toch noodzakelijk zijn om hiervoor persoonlijke gegevens te gebruiken. In het geval dergelijke AI modellen moeten worden getraind met persoonlijke gegevens, zullen deze worden toegevoegd aan dit privacybeleid en zal de mogelijkheid worden bekeken om hier een opt out aan te bieden.

Om te valideren of deze agent assist een goede transcriptie heeft gemaakt kan het noodzakelijk zijn om in de ontwikkelingsfase de opnames te beluisteren en te vergelijken met de transcriptie. Hebt u dit liever niet, dan biedt Telenet group u het recht om af te zien van het gebruik van uw recordings voor dit doeleinde (een opt out). Zie hieronder titel VIII (privacyrechten) om te lezen hoe u het recht op verzet kan uitoefenen.

Omdat het gebruik van AI-tools nieuw is, is het noodzakelijk om coaching te krijgen op het gebied van prompts. De AI-bot op het Genius-platform verbetert de manier waarop de callcentermedewerkers de meest optimale antwoorden vinden in de Genius-artikelen. Een overzicht van de prompts die door de callcentermedewerkers worden gebruikt, kan door de teamcoach worden opgevraagd om te coachen in betere prompting.

Ga voor meer informatie over het gebruik van AI naar de speciale AI-pagina op Tellit (Alles wat u moet weten over GenAI) en het AI-beleid (Search Policy Documents).

5. PREVENTIE VAN DATALEKKEN, BEHEER VAN KWETSBAARHEDEN EN MALWARE

Gespecialiseerde software kan op alle systemen worden geïnstalleerd of aangesloten om potentiële beveiligingsproblemen en risico's op gegevenslekken in realtime te detecteren.

Deze software geeft waarschuwingen over geïdentificeerde kwetsbaarheden of bedreigingen, waardoor we deze snel en effectief kunnen aanpakken. Monitoring wordt over het algemeen op een globale en niet-individuele manier uitgevoerd. Individuele controles kunnen echter worden uitgevoerd in specifieke omstandigheden, zoals het voorkomen van illegale of lasterlijke handelingen, het beschermen van de economische belangen van de onderneming en het waarborgen van de veiligheid en de goede werking van de systemen van de onderneming. Dit omvat bijvoorbeeld:

- IP-logging en blokkering van vertrouwde/verdachte locaties of IP-ranges;
- Webmonitoring om virusinfecties, misbruik en datalekken te blokkeren, op te sporen en te onderzoeken;
- Monitoring om virusinfecties, misbruik en datalekken op te sporen en te onderzoeken;
- Virusscanning van e-mail;
- Toezicht houden op het e-mailgebruik om te controleren of interne e-mails worden doorgestuurd naar persoonlijke adressen;
- E-mailanalyse bij verdenking van fraude of wetsovertreding;
- Gebruik van datalekpreventie-mogelijkheden op Telenet group-applicaties om misbruik en datalekken op te sporen;

IV. HOE BESCHERMEN WIJ UW PERSOONSGEGEVENS?

Wij nemen passende maatregelen om de persoonsgegevens die wij gebruiken te beschermen. Daartoe hebben wij technische en organisatorische beveiligingsmaatregelen geïmplementeerd om de persoonsgegevens in onze systemen en databases zoveel mogelijk te beschermen tegen ongeoorloofde toegang en/of gebruik, verlies of diefstal. Deze maatregelen worden regelmatig getest, geëvalueerd en waar nodig aangepast om te allen tijde een adequaat beveiligingsniveau te garanderen.

Ons informatiebeveiligingsbeleid is volledig gebaseerd op de internationale ISO 27002-norm en bevat richtlijnen met betrekking tot toegangscontrole, gegevensversleuteling, beveiliging van operaties, beveiliging van communicatie, fysieke beveiliging, enz. Een gespecialiseerd beveiligingsteam staat in voor de implementatie en opvolging van de richtlijnen, zodat de veiligheid van onze databanken, netwerken, infrastructuur en informatiesystemen gegarandeerd blijft.

De ontwikkeling of implementatie van nieuwe systemen, applicaties of nieuwe producten wordt ontworpen met de hoogste veiligheid in het achterhoofd, en altijd rekening houdend met uw privacy (het 'privacy by design' principe). Onze beveiligings- en privacy-experts werken nauw samen met de

ontwikkelingsteams om ervoor te zorgen dat de juiste bescherming aanwezig is, in verhouding tot het risico dat gepaard gaat met de verwerking van de persoonsgegevens.

Toegangscontrole is een belangrijk aspect van ons informatiebeveiligingsbeleid. Telenet group heeft procedures geïmplementeerd om de toegang tot onze databases, systemen, apparatuur en netwerken te beperken tot die personen die deze toegang strikt nodig hebben om hun functie uit te voeren. Deze personen moeten een strikte geheimhoudingsplicht in acht nemen en zich houden aan alle richtlijnen om de bescherming van persoonsgegevens te waarborgen. De toegang tot de gegevens van onze medewerkers in hun personeelsdossier is beperkt tot HR en management op een "need-to-know" basis. Met betrekking tot elektronische informatie moeten gebruikers zich authenticeren en een wachtwoord invoeren voordat toegang wordt verleend. Geprinte bestanden van medewerkers worden opgeborgen in afsluitbare kasten in het HR-kantoor.

Telenet group biedt ook privacy- en security-specifieke opleidingen aan voor zijn medewerkers, om de richtlijnen en procedures te verduidelijken voor zijn medewerkers en hen bewust te maken van de risico's die gepaard gaan met de verwerking van persoonsgegevens.
Telenet group legt ook hoge veiligheidseisen op aan zijn partners en leveranciers die in onze opdracht jouw persoonsgegevens verwerken. Mede door middel van contractuele garanties zorgen wij ervoor dat zij, net als wij, uw gegevens veilig en met respect voor de privacywetgeving verwerken. We verwachten dan ook van onze partners en leveranciers dat ze een informatiebeveiligingsbeleid en beveiligingsmaatregelen implementeren die geënt zijn op internationale standaarden en best practices.

V. GEVEN WIJ UW PERSOONSGEGEVENS DOOR? AAN WIE?

Uw persoonsgegevens kunnen worden gedeeld met de volgende partijen:

DERDEN DIE DIENSTEN VERLENEN AAN TELENET GROUP EN DIE IN ONZE NAAM HANDELEN

Uw persoonsgegevens kunnen door onze leveranciers worden gebruikt voor dezelfde doeleinden als hierboven vermeld. Het spreekt voor zich dat wij alleen de persoonsgegevens verstrekken of toegankelijk maken die de leverancier nodig heeft om de dienst te verlenen en dat zij uw persoonsgegevens namens ons verwerken.

Hier zijn een paar voorbeelden:

- Het sociaal secretariaat dat in onze opdracht de loonadministratie uitvoert;
- Talentplatforms die ons helpen jouw vaardigheden in kaart te brengen;
- Aanbieders van digitale werkplekken (zoals Microsoft Office, enz.);
- Bedrijven gespecialiseerd in ICT-ondersteuning en cybersecurity;
- Bedrijven die training voorzien;
- De bedrijven die verantwoordelijk zijn voor de toegangscontrole en beveiliging in de gebouwen;
- Bedrijven die ons helpen met het bezorgen van geschenken aan onze werknemers;
- Bedrijven die ons helpen bij het organiseren van evenementen voor onze werknemers;

- Het document beheer (en bewaring) platform Doccle (Deze gegevens worden verwerkt met het oog op het automatisch versturen van uw loonbrieven en fiscale documenten naar uw Doccle-account, voor bewaring van deze documenten. Hou er rekening mee dat Telenet group niet betrokken of verantwoordelijk is voor de verdere bewaring en toegankelijkheid van je arbeidsdocumenten op/via je individuele Doccle-account, die langer zal duren dan de beëindiging van je arbeidsrelatie met Telenet group. Deze verdere verwerking van je persoonsgegevens valt onder de verantwoordelijkheid en controle van Doccle en is onderworpen aan de voorwaarden van Doccle, met inbegrip van haar Privacybeleid).

DOORGIFTE VAN PERSOONSGEGEVENS AAN DERDEN DIE NIET NAMENS ONS WERKEN (DIE OPTREDEN ALS VERWERKINGSVERANTWOORDELIJKEN)

Wij kunnen uw gegevens ook doorgeven aan andere bedrijven die hun eigen doeleinden voor de verwerking van uw gegevens bepalen. Dit impliceert dat hun privacybeleid van toepassing is.

Hier zijn enkele voorbeelden:

- Aanbieders van tank- en laadkaarten (bijv. Eneco, Blossom, Total);
- Leasing- en verhuurbedrijven (bijv. Arval, Blue Bike). Leasemaatschappijen verzamelen en verwerken een groot aantal gegevens over uw gebruik van de bedrijfsauto (zoals locatiegegevens, gebruiksgegevens enz.). Bekijk hun privacybeleid;
- Verzekeringsmaatschappijen (bijv. Van Breda);
- Pensioenfondsen (bv. het pensioenfonds Telenet group, IPB genaamd, verwerkt uw persoonsgegevens om uw aanvullende pensioenrechten te beheren);
- Oplaadpunten voor elektrische auto's;
- SKIPR kaart (mobiliteit);
- Degroof Petercam;
- Ecocheques, maaltijdcheques (Sodexo, Edenred, Monizze);
- Zakelijke reisbureaus.

ONZE KLANTEN EN PARTNERS

In het kader van onze normale bedrijfsactiviteiten ontvangen onze partners (klanten of alle personen die gebruik maken van onze diensten, leveranciers en andere (potentiële) contractpartijen), met wie u samenwerkt in de hoedanigheid van werknemer, uw zakelijke contactgegevens die nodig zijn voor dergelijke activiteiten.

IN HET KADER VAN MOGELIJKE REORGANISATIES EN OVERNAMES

Uw persoonsgegevens kunnen ook geraadpleegd worden door derden die betrokken zijn bij dergelijke mogelijke transacties (bijvoorbeeld in het kader van een zogenaamde "due diligence"), en dit uitsluitend met het oog op een dergelijke transactie. In een dergelijk geval is de doorgifte van de

relevante gegevens gebaseerd op het gerechtvaardigd belang van Telenet group, haar aandeelhouders en de betrokken derden met het oog op de voorgenomen transactie.

OM TE VOLDOEN AAN WETTELIJKE VEREISTEN

Persoonsgegevens kunnen ook aan andere derden worden verstrekt om te voldoen aan wettelijke vereisten, zoals:

- De belastingdienst;
- Instellingen voor sociale zekerheid;
- Arbeidsinspectiediensten;
- Preventieadviseurs;
- Deurwaarders.

INTERNATIONALE DOORGIFTE VAN GEGEVENS

Uw persoonsgegevens worden ook buiten de Europese Unie (de Europese Economische Ruimte, ook wel EER genoemd) verwerkt. Het is een feit dat veel grote IT-leveranciers, infrastructuuraanbieders en technologiebedrijven niet in de Europese Unie zijn gevestigd.

Enkele voorbeelden:

- IT-beveiliging – VS (Crowdstrike);
- Ondersteuning en onderhoud – India (Cognizant);
- Digitale werkplek – VS (Microsoft);
- Training, L&D – US (Datacamp);
- Gegevensopslag in de cloud - VS (AWS).

Bij het doorgeven van uw persoonsgegevens buiten de EER respecteren wij steeds de vereisten van de privacywetgeving inzake internationale doorgiften:

- We kunnen persoonsgegevens doorgeven aan landen waarvan de Europese Commissie heeft vastgesteld dat ze een adequaat niveau van gegevensbescherming bieden in overeenstemming met de Europese privacywetgeving (AVG), en
- We kunnen persoonsgegevens overdragen op basis van de relevante modules van de modelcontractbepalingen van de Europese Commissie.

Bovendien hebben we ons afgestemd op de richtlijnen voor internationale gegevensoverdracht die zijn uitgevaardigd door het Europees Comité voor gegevensbescherming. Voor elke internationale doorgifte voeren we een Data Transfer Impact Assessment uit om de wetgeving van de derde landen te beoordelen en eventuele praktijken te identificeren die onverenigbaar zijn met de verplichtingen van het doorgiftemechanisme. Deze analyse stelt ons ook in staat om aanvullende beveiligings-, contractuele en organisatorische maatregelen te identificeren om de gegevens te beschermen tegen ongeoorloofde toegang door de overheidsinstanties van het derde land.

VI. Hoe lang bewaren wij uw Persoonsgegevens?

Wij bewaren uw persoonsgegevens zolang als nodig is voor de doeleinden die in dit privacybeleid zijn uiteengezet. Over het algemeen worden persoonsgegevens bewaard voor de gehele duur van het dienstverband, hetzij op grond van een arbeidsovereenkomst, hetzij een overeenkomst van opdracht. Na de beëindiging van het dienstverband moet Telenet group persoonsgegevens nog bewaren gedurende een periode die afhankelijk is van het verwerkingsdoel. Nadat de toepasselijke bewaartermijn(en) is verstreken, worden de persoonsgegevens verwijderd of geanonimiseerd.

Voorbeelden: Telenet group is wettelijk verplicht om alle gegevens die deel uitmaken van het personeelsregister te bewaren voor een periode van 5 jaar**.**

VII. Maken wij gebruik van zogenaamde "geautomatiseerde individuele besluitvorming"?

Wij maken in principe geen gebruik van dergelijke geautomatiseerde individuele besluitvorming. Indien een dergelijke geautomatiseerde besluitvorming in de toekomst zou worden gebruikt, zal deze in overeenstemming met de AVG worden geïmplementeerd en zal ervoor worden gezorgd dat de rechten van de werknemers te allen tijde worden gewaarborgd.

VIII. De privacyrechten van onze medewerkers

Op basis van de AVG heeft u de volgende rechten in verband met de verwerking van uw persoonsgegevens door Telenet group. Deze rechten zijn niet absoluut en de uitoefening ervan kan onderworpen zijn aan bepaalde voorwaarden en uitzonderingen, zoals bepaald in de AVG.

UW RECHT OP INZAGE

U heeft het recht om op elk moment van Telenet group te weten of wij uw persoonsgegevens al dan niet verwerken, en, indien wij uw gegevens verwerken, om die gegevens in te zien en aanvullende informatie over de verwerking te ontvangen. U heeft ook het recht om een gratis kopie van de verwerkte gegevens in een begrijpelijke vorm te ontvangen. Telenet group kan een redelijke vergoeding vragen om de administratieve kosten te dekken van elke extra kopie die u aanvraagt. Indien de toegang tot de persoonsgegevens wordt geweigerd, zal de reden hiervan worden meegedeeld.

UW RECHT OP CORRECTIE VAN PERSOONSGEGEVENS

U heeft het recht om onvolledige, onjuiste, ongepaste of verouderde gegevens onmiddellijk te laten corrigeren. Om uw gegevens up-to-date te houden, vragen wij u in ieder geval om ons op de hoogte te brengen van eventuele wijzigingen, zoals een verhuis, een wijziging van e-mailadres of de vernieuwing van uw identiteitskaart. Deze wijzigingen kunnen worden doorgegeven via een RM-ticket.

UW RECHT OP VERGETELHEID (HET 'RECHT OP VERGETELHEID')

U heeft het recht om uw persoonsgegevens te laten verwijderen in de volgende gevallen:

- Uw persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor ze door Telenet group zijn verzameld of anderszins verwerkt;
- U trekt uw voorafgaande toestemming voor de verwerking in, en er is geen andere rechtsgrond waarop Telenet group zich zou kunnen beroepen voor de (verdere) verwerking;
- U maakt bezwaar tegen de verwerking van uw persoonsgegevens en er zijn geen zwaarwegende, gerechtvaardigde gronden meer voor de (verdere) verwerking door Telenet group;
- Uw persoonsgegevens worden op onrechtmatige wijze verwerkt;
- Uw persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting;
- Uw persoonsgegevens zijn verzameld toen u nog minderjarig was.

Houd er echter rekening mee dat we niet altijd in staat zijn om alle gevraagde persoonsgegevens te verwijderen, bijvoorbeeld als de verwerking van deze gegevens noodzakelijk is om te voldoen aan onze wettelijke verplichtingen.

UW RECHT OP BEPERKING VAN DE VERWERKING

U heeft het recht om de beperking van de verwerking van uw persoonsgegevens te verkrijgen als een van de volgende aspecten van toepassing is:

- U betwist de juistheid van deze persoonsgegevens: het gebruik wordt beperkt gedurende een periode die lang genoeg is om Telenet group in staat te stellen de juistheid van de gegevens na te gaan;
- Uw persoonsgegevens worden op een onrechtmatige manier verwerkt: in plaats van uw gegevens te wissen, kunt u vragen om het gebruik ervan te beperken;
- Telenet group heeft uw gegevens niet langer nodig voor de oorspronkelijke verwerkingsdoeleinden, maar heeft ze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering: in plaats van het wissen van uw gegevens, wordt het gebruik ervan beperkt tot de instelling, uitoefening of onderbouwing van de rechtsvordering;
- Zolang er nog geen beslissing is genomen over de uitoefening van uw recht om zich te verzetten tegen de verwerking, kunt u de beperking van het gebruik van uw persoonsgegevens vragen.

UW RECHT OM BEZWAAR TE MAKEN TEGEN DE VERWERKING VAN UW PERSOONSGEGEVENS.

U heeft het recht om u te verzetten tegen de verwerking van uw persoonsgegevens op basis van uw specifieke situatie indien de verwerking plaatsvindt in het kader van een gerechtvaardigd belang van Telenet group, of in het kader van het algemeen belang. Telenet group zal de verwerking van uw persoonsgegevens staken, tenzij het dwingende en gerechtvaardigde gronden voor de verwerking kan aantonen die zwaarder wegen dan uw redenen, of indien de verwerking van de persoonsgegevens verband houdt met het instellen, uitoefenen of onderbouwen van een rechtsvordering (bijvoorbeeld het indienen van een verzoek bij een rechtbank).

UW RECHT OP OVERDRAAGBAARHEID VAN PERSOONSGEGEVENS, OF DATAPORTABILITEIT"

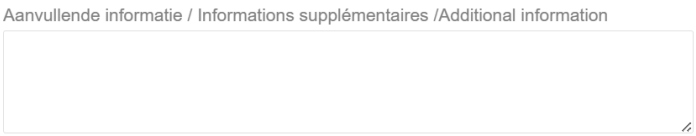
U heeft het recht om uw persoonsgegevens te 'recupereren', bijvoorbeeld als u van werkgever zou veranderen. Dit kan enkel voor de persoonsgegevens die u zelf aan Telenet group hebt verstrekt, op basis van toestemming of na akkoord. In alle andere gevallen zult u dit recht niet kunnen uitoefenen (bijvoorbeeld als de verwerking van uw gegevens plaatsvindt op basis van een wettelijke verplichting).

Dit recht omvat 2 aspecten:

- U kunt Telenet group vragen om de betreffende persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm aan u terug te bezorgen; en
- U kan Telenet group vragen om de persoonsgegevens rechtstreeks over te dragen aan een andere verwerkingsverantwoordelijke. U bent daarbij zelf verantwoordelijk voor de juistheid en veiligheid van het (e-mail)adres dat u opgeeft voor de overdracht. Telenet group heeft het recht om dit te weigeren indien de doorgifte technisch niet mogelijk is.

HOE KAN IK MIJN PRIVACYRECHTEN UITOEFENEN?

U kunt uw privacyrechten uitoefenen via de online Privacy pagina op het intranet Tellit: Privacy van medewerkers (sharepoint.com). Formuleer welk recht u wilt uitoefenen in het veld aanvullende informatie:



Zijn hier kosten aan verbonden? U kunt uw privacyrechten kosteloos uitoefenen, tenzij uw verzoek kennelijk ongegrond of buitensporig is, met name als het repetitief van aard is. In overeenstemming met de privacywetgeving hebben wij in een dergelijk geval en naar eigen goeddunken het recht (i) u een redelijke vergoeding in rekening te brengen (rekening houdend met de administratieve kosten die gemoeid zijn met het verstrekken van de gevraagde informatie of communicatie, alsook de kosten die gepaard gaan met het implementeren van de gevraagde maatregelen), of (ii) te weigeren aan uw verzoek te voldoen.

In welk formaat krijg ik antwoord? Als u uw verzoek elektronisch indient, worden de gegevens ook elektronisch verstrekt, indien dit mogelijk is en tenzij u anders verzoekt. Wij zullen u in ieder geval een beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk antwoord geven.

Wanneer krijg ik antwoord? Wij zullen zo snel mogelijk, en in ieder geval binnen een maand na ontvangst van uw verzoek, op uw verzoek reageren. Afhankelijk van de complexiteit van de

verzoeken en het aantal verzoeken kan deze termijn indien nodig met nog eens twee maanden worden verlengd. Als de reactietermijn wordt verlengd, zullen wij u hiervan binnen een maand na ontvangst van het verzoek op de hoogte stellen.

Wat gebeurt er als Telenet group niet aan mijn verzoek voldoet? In ons antwoord zullen wij u altijd informeren over de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit en om in beroep te gaan bij de rechtbank.

Wat als ik geen toegang heb tot Tellit? Dan kan je je vraag doorsturen naar privacy@telenet group.be. Weet dat er een bijkomende identificatiecheck dient plaats te vinden.

IX. Hoe kan ik Telenet group contacteren over mijn privacy?

- Ik wil mijn privacyrechten uitoefenen

U kunt uw rechten uitoefenen door een verzoek in te dienen via een formulier/supportticket op Privacy van medewerkers (sharepoint.com)

- Ik wil een privacyschending melden bij de Functionaris Gegevensbescherming

U kunt een privacyschending melden via de Privacy Incident First Aid Kit (sharepoint.com)

- Ik heb een andere vraag over de verwerking van mijn persoonsgegevens

U kunt uw vraag stellen via het formulier over privacy van werknemers (sharepoint.com) of door rechtstreeks contact op te nemen met uw HR Business Partner.

U kunt uw vraag, klacht of verzoek ook per brief sturen ter attentie van de Functionaris voor gegevensbescherming (of "DPO"):
Telenet BV, Liersesteenweg 4, 2800 Mechelen of gebruik het e-mailadres privacy@telenet group.be

X. Aanpassingen aan dit Privacybeleid

Telenet group kan dit Privacybeleid op elk moment herzien, bijvoorbeeld naar aanleiding van (i) nieuwe of gewijzigde wetgeving, regels en voorschriften, met inbegrip van aanbevelingen van de Gegevensbeschermingsautoriteit of andere overheidsinstanties zoals bijvoorbeeld het BIPT, of (ii) wijzigingen in de activiteiten en processen van Telenet group.

XI. Escalatie naar de toezichthoudende autoriteit

De Gegevensbeschermingsautoriteit is een onafhankelijke instantie die erop toeziet dat uw persoonsgegevens in overeenstemming met de wet worden verwerkt. Indien u een klacht heeft in verband met de verwerking van uw persoonsgegevens door Telenet group, of indien u een procedure tot bemiddeling wenst op te starten, kan u contact opnemen met de Gegevensbeschermingsautoriteit via

https://www.gegevensbeschermingsautoriteit.be/burger/acties/klacht-indienen.

Laatste update: Januari 2025