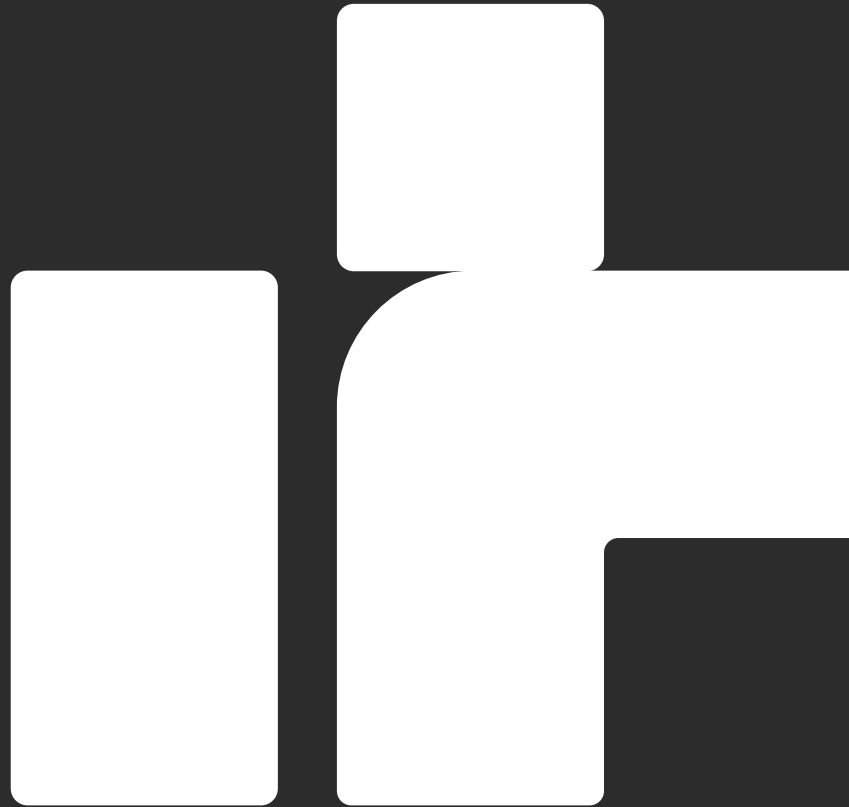


Privacyreglement

December 2025



Inhoud

Doel en toepassingsgebied

1. Persoonsgegevens die wij verzamelen
2. Hoe wij persoonsgegevens verzamelen
3. Doeleinden van verwerking
4. Bewaartermijnen
5. Persoonsgegevens van oud-medewerkers
6. Beveiliging van persoonsgegevens
7. Monitoring en transparantie
8. Delen van gegevens met externe partijen
9. Internationale doorgifte van gegevens
10. Jouw rechten
11. Vragen en contact
12. Wijzigingen

Doel en toepassingsgebied

Dit interne privacybeleid beschrijft welke persoonsgegevens IT Building van jou (als medewerker) verzamelt, op welke wijze deze gegevens worden verzameld, gebruikt en verwerkt, en hoe IT Building voldoet aan zijn wettelijke verplichtingen op dit gebied. Ook geeft het beleid een overzicht van de organisatorische en technische maatregelen die zijn geïmplementeerd om jouw persoonsgegevens te beschermen en hoe wij de richtlijnen van de Algemene Verordening Gegevensbescherming (AVG) naleven. Dit beleid (en de daarin beschreven maatregelen) maakt deel uit van het Information Security Management System (ISMS) van IT Building en wordt regelmatig onderhouden en gecontroleerd.

Dit beleid is van toepassing op alle (kandidaat)medewerkers van IT Building, inclusief tijdelijke krachten, stagiairs, freelancers en andere personen die werkzaamheden voor ons verrichten. Waar in dit document gesproken wordt over “medewerkers”, worden al deze categorieën bedoeld. Het beleid omvat eveneens de verwerking van persoonsgegevens van oud-medewerkers (zie Sectie 5). IT Building heeft een Functionaris Gegevensbescherming (FG) aangewezen die toezicht houdt op de naleving van de privacywetgeving en dit beleid. Vragen of verzoeken omtrent privacy kunnen bij de FG of via HR worden ingediend (zie Sectie 11).

1. Persoonsgegevens die wij verzamelen

IT Building verzamelt en bewaart verschillende categorieën van persoonsgegevens over medewerkers, in overeenstemming met de toepasselijke wetgeving. Het gaat onder meer om:

- Basisgegevens: naam, (e-mail)adres, telefoonnummer.
- Identificatiegegevens: geboortedatum, nationaliteit, burgerservicenummer (BSN) of sofinummer.
- Werkgerelateerde gegevens: functietitel, afdeling, standplaats, werkrooster, salaris en belastinginformatie.
- Opleiding en kwalificaties: behaalde diploma's, certificaten en andere relevante kwalificaties.

IT Building verzamelt deze informatie uitsluitend indien dit noodzakelijk is voor de uitvoering van de werkgeversverplichtingen en in overeenstemming met de geldende privacywetgeving. In principe verwerken wij geen bijzondere categorieën van persoonsgegevens (zoals gegevens over gezondheid, religie of lidmaatschap van een vakbond), tenzij dit wettelijk vereist is of met jouw uitdrukkelijke toestemming gebeurt.

2. Hoe wij persoonsgegevens verzamelen

Afhankelijk van het type gegevens en het doel van verwerking, kunnen persoonsgegevens op verschillende manieren bij IT Building worden verzameld:

- Sollicitatieproces: tijdens werving en selectie ontvangen we gegevens van sollicitanten, zoals CV's, motivatiebrieven en referenties, om geschiktheid voor een functie te beoordelen.
- Formulieren bij indiensttreding: nieuwe medewerkers verstrekken persoonlijke informatie (bijv. NAW-gegevens, contactinformatie, burgerlijke staat, etc.) via inschrijfformulieren of HR-systemen.
- Wettelijke formulieren: medewerkers verstrekken fiscale en administratieve gegevens (bijv. loonbelastingverklaringen) zodat IT Building kan voldoen aan wet- en regelgeving, zoals het juist inhouden van belastingen.

- Screening en verificatie: indien van toepassing kan IT Building achtergrondscreenings uitvoeren (bijv. identiteits- en referentiecontroles, verificatie van opleiding of werkervaring, en eventueel controle op strafrechtelijke veroordelingen) om de integriteit en veiligheid binnen het bedrijf te waarborgen.

Daarnaast kunnen tijdens het dienstverband gegevens worden gegenereerd of verzameld, bijvoorbeeld via beoordelingsgesprekken, verlofregistraties, tijdschrijven, gebruik van bedrijfsmiddelen en correspondentie. Deze gegevens worden in de personeelsadministratie opgenomen en volgens dit beleid behandeld.

3. Doeleinden van verwerking

IT Building verwerkt persoonsgegevens van medewerkers voor uiteenlopende doeleinden, waaronder:

- Wettelijke verplichtingen: Om te voldoen aan wet- en regelgeving dient IT Building bepaalde medewerkersgegevens te verzamelen en bij te houden (zoals voor belastingwetten en arbeidswetten).
Personeelsadministratie en bedrijfsvoering: Voor een correcte HR-administratie en uitvoering van de arbeidsovereenkomst verwerkt IT Building persoonsgegevens zoals loon- en salarisgegevens, arbeidsovereenkomsten, functiewijzigingen, prestatieverslagen, verlof- en verzuimregistraties, etc.. Deze gegevensverwerking is nodig voor onder andere salarisbetaling, beoordelings- en ontwikkelingsprocessen, training en opleiding, en algemene bedrijfsvoering.

- Veiligheid en beveiliging: IT Building verwerkt persoonsgegevens om de veiligheid van de werkomgeving te garanderen en bedrijfsmiddelen te beschermen. Ook worden gegevens verwerkt om ongeautoriseerde toegang, fraude of ander misbruik te voorkomen en te detecteren, en om incidenten adequaat af te handelen.

Indien IT Building persoonsgegevens voor andere, onverenigbare doeleinden wil gebruiken, zal hiervoor waar nodig toestemming worden gevraagd of een andere rechtsgrond worden aangetoond conform de AVG. IT Building verwerkt geen persoonsgegevens voor doeleinden die niet verenigbaar zijn met de oorspronkelijke redenen waarvoor ze zijn verzameld, tenzij een uitzonderingsgrond van toepassing is.

4. Bewaartermijnen

IT Building bewaart persoonsgegevens niet langer dan noodzakelijk is voor de hierboven genoemde doeleinden of zoals wettelijk vereist. Bij het bepalen van bewaartermijnen houden wij rekening met relevante wet- en regelgeving:

- Belastingwetgeving: Financiële administratie, waaronder salarisgegevens, moet 7 jaar bewaard worden.
- Arbeidswetgeving: Bepaalde personeelsgegevens (bijv. arbeidsovereenkomst, personeelsdossier) worden bewaard gedurende de duur van de arbeidsovereenkomst en tot 2 jaar na beëindiging van het dienstverband.

- AVG (Algemene Verordening Gegevensbescherming): Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel waarvoor ze zijn verzameld of verwerkt.

Na afloop van de toepasselijke bewaartermijn zorgt IT Building ervoor dat de betreffende persoonsgegevens veilig worden verwijderd of geanonimiseerd. Tijdens de bewaartermijnen worden passende technische en organisatorische maatregelen genomen om de gegevens beveiligd te houden (zie Sectie 6).

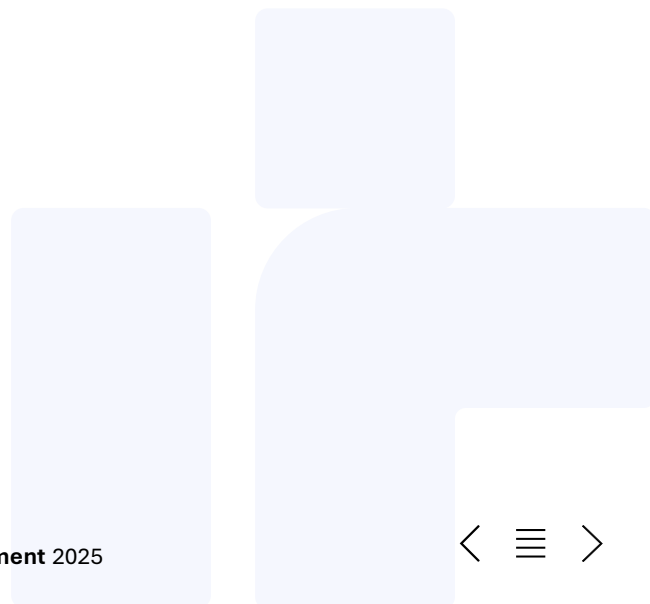
5. Persoonsgegevens van oud-medewerkers

Ook nadat een medewerker uit dienst is, gaat IT Building zorgvuldig om met diens persoonsgegevens. Bij beëindiging van het dienstverband worden personeelsdossiers en relevante gegevens gedeeltelijk behouden voor zover noodzakelijk voor onderstaande doelen:

- Wettelijke en contractuele verplichtingen: IT Building moet voldoen aan verplichtingen die voortvloeien uit het vroegere dienstverband, zoals het afhandelen van laatste loonbetalingen, pensioenrechten of uitkeringsaanspraken (bijv. informatie voor het UWV met betrekking tot WW of ziektewet). Ook wettelijke bewaarplichten (zie Sectie 4) blijven van toepassing.
- Afhandelen van verzoeken en geschillen: Persoonsgegevens van oud-medewerkers worden bewaard om eventuele latere vragen, verzoeken of claims te kunnen behandelen. Denk hierbij aan het verstrekken van werkverklaringen/referenties op verzoek van de oud-medewerker, of het behandelen van arbeidsrechtelijke geschillen, klachten, disciplinaire zaken of juridische procedures waarin de oud-medewerker betrokken is.
- Operationele continuïteit: Om de continuïteit van de bedrijfsvoering te waarborgen kan het nodig zijn bepaalde gegevens te bewaren. Bijvoorbeeld om de overdracht van kennis en dossiers mogelijk te maken, dienstverlening aan klanten te blijven voorzien, of om toegang te behouden tot zakelijke communicatie (zoals e-mails of documenten van de oud-medewerker) voor zover noodzakelijk voor legitieme bedrijfsdoeleinden.

5. Persoonsgegevens van oud-medewerkers

Tijdens de periode dat gegevens van oud-medewerkers worden bewaard, blijven de privacyrechten (zie Sectie 11) van kracht. IT Building zal geen nieuwe verwerkingen uitvoeren met oud-werknemersgegevens die onverenigbaar zijn met bovengenoemde doeleinden. Gegevens die niet langer nodig zijn, worden tijdig verwijderd volgens de vastgestelde termijnen.



6. Beveiliging van persoonsgegevens

IT Building neemt strikte beveiligingsmaatregelen om persoonsgegevens te beschermen tegen verlies, ongevoegde inzage, ongeautoriseerde gebruik of openbaarmaking. Enkele belangrijke maatregelen die wij hanteren zijn:

- Beperkte toegang: Toegang tot personeelsgegevens is beperkt tot geautoriseerde personen (zoals HR-functionarissen en directie) die deze informatie nodig hebben voor hun taken. Toegangsbeveiliging wordt afgedwongen met sterke wachtwoorden, multi-factor authenticatie en strikte gebruikersrechten.
- Beveiligingsbeleid en procedures: IT Building beschikt over interne informatiebeveiligingsbeleid en procedures om het gebruik van (persoons)gegevens te beheersen.

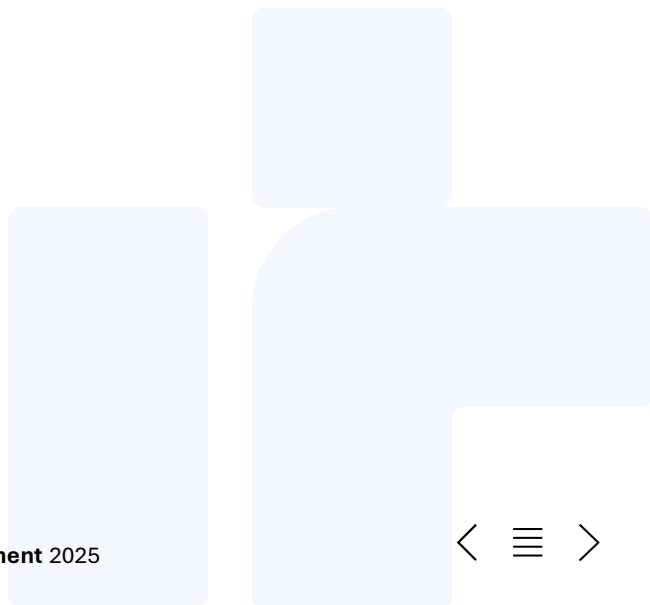
Onder andere zijn er richtlijnen voor toegangscontrole, incidentmanagement, veilige opslag, gebruik van versleuteling, en periodieke controle van naleving. Medewerkers dienen deze beleidsregels na te leven om de gegevensveiligheid te garanderen.

- Bewustwording en training: Medewerkers worden periodiek getraind en bewust gemaakt van de risico's en best practices rondom privacy en gegevensbescherming. Voorbeelden van onderwerpen zijn het veilig omgaan met wachtwoorden, herkennen van phishing-pogingen, en het beveiligen van apparatuur zoals laptops. Door deze bewustwordingsprogramma's wordt het risico op menselijke fouten verkleind en de algehele beveiliging van persoonsgegevens vergroot.

6. Beveiliging van persoonsgegevens

- Audits en toezicht: IT Building voert periodieke audits, controles en monitoring uit om te toetsen of privacy- en beveiligingsmaatregelen effectief zijn en worden nageleefd. Eventuele risico's of zwakke plekken worden hierbij geïdentificeerd en aangepakt. Waar nodig worden verbeteringen doorgevoerd om de bescherming van persoonsgegevens continu te optimaliseren.

Alle beveiligingsmaatregelen worden regelmatig geëvalueerd en waar nodig aangepast aan nieuwe risico's, technische ontwikkelingen of veranderende wetgeving. Ook externe partijen die voor ons persoonsgegevens verwerken (zie Sectie 9) moeten passende beveiligingsmaatregelen in acht nemen.



7. Monitoring en transparantie

IT Building respecteert de privacy van medewerkers en voert geen stelselmatige, persoonsgerichte monitoring uit van werknemers zonder legitieme aanleiding. Er is geen actieve monitoring op individueel niveau van bijvoorbeeld e-mail, bestanden of surfgedrag, tenzij dit noodzakelijk is om dringende redenen (zoals een gerechtvaardigd vermoeden van fraude, misbruik of andere ernstige overtredingen). Wel maken wij gebruik van geautomatiseerde beveiligingssystemen die het IT-netwerk en bedrijfsapparatuur bewaken op verdachte activiteiten, virussen of ongeautoriseerde toegang. Deze systemen monitoren het gebruik van onze IT-voorzieningen in algemene zin, maar niet gericht op persoonlijke inhoud van medewerkers zonder specifieke aanleiding.

Indien het toch noodzakelijk wordt geacht om gericht gegevens van of over een medewerker te controleren (bijvoorbeeld inzage in e-mailcorrespondentie in het kader van een onderzoek), zal dit altijd gebeuren in overeenstemming met de wet, na interne goedkeuring door de directie en/of de FG, en met inachtneming van het proportionaliteits- en subsidiariteitsbeginsel. IT Building zal waar mogelijk transparant zijn over eventuele maatregelen die impact hebben op de privacy van medewerkers. Beleidswijzigingen of nieuwe vormen van gegevensverwerking die significante gevolgen hebben voor medewerkers, zullen tijdig gecommuniceerd worden. Medewerkers kunnen bij vragen over monitoring of privacy altijd terecht bij de contactpersonen genoemd in dit beleid (zie Sectie 11).

8. Delen van gegevens met externe partijen

IT Building deelt jouw persoonsgegevens alleen met derden (externen) voor zover dat noodzakelijk is voor de uitvoering van de arbeidsovereenkomst, de bedrijfsvoering, of om te voldoen aan een wettelijke verplichting. In alle gevallen zorgen wij ervoor dat er passende waarborgen bestaan om jouw gegevens te beschermen. Enkele voorbeelden van externe partijen waarmee wij persoonsgegevens (indien nodig) kunnen uitwisselen:

- **Dienstverleners:** Externe leveranciers die diensten aan IT Building verlenen, zoals salarisadministratie, boekhouding, IT- en cloudproviders, arbodiensten, trainingsbureaus of recruitmentbureaus. Zij krijgen uitsluitend toegang tot relevante gegevens voor zover nodig voor hun dienstverlening.
- **Overheidsinstanties en toezichthouders:** Bijvoorbeeld de Belastingdienst, UWV, pensioenuitvoerders, of toezichthoudende autoriteiten, maar alleen voor zover wettelijke voorschriften dit vereisen.

- **Klanten of zakenpartners:** In beperkte gevallen kan het voorkomen dat basiscontactgegevens van een medewerker worden gedeeld met een klant of partner, bijvoorbeeld omdat die medewerker bij een project voor die klant betrokken is of op locatie werkzaamheden verricht.

Met alle externe partijen die namens of samen met ons persoonsgegevens verwerken, maakt IT Building afspraken om de privacy te waarborgen. Wanneer deze partijen als verwerker optreden, sluiten wij verwerkersovereenkomsten die hen verplichten vertrouwelijk met de data om te gaan en adequate technische en organisatorische beveiligingsmaatregelen te treffen.

8. Delen van gegevens met externe partijen

We verplichten zulke dienstverleners de persoonsgegevens uitsluitend volgens onze instructies en in overeenstemming met de wet te verwerken. In gevallen waarin externe partijen zelf (mede)verwerkingsverantwoordelijke zijn (bijv. overheden), delen wij gegevens alleen op basis van een wettelijke grondslag en zorgen we voor een passende rechtmatigheidstoets.

IT Building zal nooit persoonsgegevens verkopen aan derden. Delen van gegevens gebeurt altijd op een zorgvuldige manier en met respect voor de privacy van onze medewerkers.

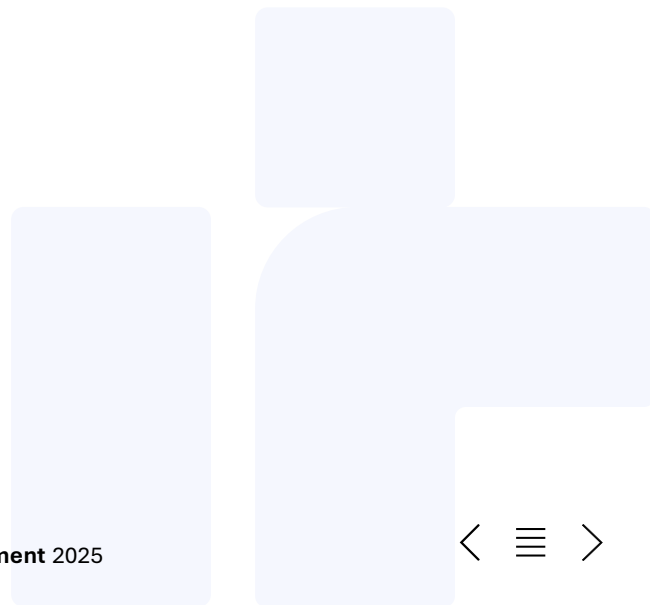
9. Internationale doorgifte van gegevens

Het kan voorkomen dat IT Building of onze externe dienstverleners persoonsgegevens opslaan of verwerken buiten Nederland, of zelfs buiten de Europese Economische Ruimte (EER). In dergelijke gevallen zorgen wij ervoor dat de internationale doorgifte voldoet aan de toepasselijke privacywetgeving. Dit betekent dat er een passend beschermingsniveau gegarandeerd wordt in het ontvangende land, vergelijkbaar met het niveau van databescherming binnen de EER.

Voorbeelden hiervan zijn het delen van persoonsgegevens met een zusterorganisatie of moedermaatschappij buiten de EU, of het gebruik van een cloud-leverancier gevestigd in de VS. IT Building neemt in dergelijke situaties adequate maatregelen, zoals het sluiten van EU-modelcontractbepalingen (Standard Contractual Clauses) of te zorgen dat de ontvangende partij gecertificeerd is onder een door de EU goedgekeurd mechanisme.

Ook zullen we voldoen aan overige relevante voorschriften uit de AVG omtrent internationale doorgifte.

Medewerkers zullen waar relevant geïnformeerd worden over de landen buiten de EER waarnaar hun gegevens eventueel worden overgebracht. Bij vragen hierover kunnen zij contact opnemen zoals aangegeven in Sectie 11.



10. Jouw rechten

Als medewerker (en daarmee betrokkene in de zin van de AVG) heb je verschillende privacyrechten ten aanzien van jouw persoonsgegevens. IT Building respecteert deze rechten en heeft procedures ingericht om tijdig op verzoeken te reageren:

- **Recht op inzage:** Je hebt het recht om te weten welke persoonsgegevens van jou worden verwerkt en om een kopie te ontvangen van die gegevens. Op verzoek zal IT Building een overzicht geven van de persoonsgegevens die van jou zijn vastgelegd en informatie over de verwerkingsdoeleinden.
- **Recht op rectificatie:** Je hebt het recht om onjuiste persoonsgegevens te laten corrigeren en om onvolledige gegevens te laten aanvullen. IT Building draagt er zorg voor dat wijzigingen zo spoedig mogelijk in alle relevante systemen worden doorgevoerd.
- **Recht op verwijdering:** Je hebt in bepaalde gevallen het recht om jouw persoonsgegevens te laten verwijderen. Dit recht, ook wel het “recht op vergetelheid” genoemd, is van toepassing als de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld, als ze onrechtmatig worden verwerkt, als je succesvol bezwaar hebt gemaakt tegen de verwerking, of indien verwijdering nodig is om te voldoen aan een wettelijke verplichting. Houd er rekening mee dat dit recht niet absoluut is – soms moet IT Building gegevens bewaren op grond van de wet (zie Sectie 5) of andere gerechtvaardigde belangen.
- **Recht op beperking van de verwerking:** Je hebt het recht om in bepaalde gevallen de verwerking van jouw persoonsgegevens te laten beperken

10. Jouw rechten

Dit betekent dat IT Building de gegevens tijdelijk niet mag verwerken (alleen opslaan), bijvoorbeeld gedurende de periode dat wordt vastgesteld of de gegevens juist zijn, of wanneer de verwerking onrechtmatig is maar je niet wilt dat de gegevens worden gewist.

- **Recht op dataportabiliteit:** Je hebt het recht om bepaalde persoonsgegevens die je aan IT Building hebt verstrekt, in een gestructureerd, gangbaar en machineleesbaar formaat te ontvangen, zodat je deze gegevens desgewenst aan een andere partij kunt overdragen. Voor zover technisch mogelijk kunnen wij dergelijke overdracht ook direct voor je faciliteren.
- Recht van bezwaar:** Je hebt het recht om bezwaar te maken tegen de verwerking van jouw persoonsgegevens in gevallen waarin de verwerking gebaseerd is op een gerechtvaardigd belang van IT Building of op een taak van algemeen belang.

Als je bezwaar maakt, staakt IT Building de betreffende verwerking, tenzij wij dwingende gerechtvaardigde gronden kunnen aantonen die zwaarder wegen dan jouw belangen, rechten en vrijheden (of die verband houden met een rechtsvordering).

Om één van deze rechten uit te oefenen, kun je een verzoek indienen volgens de procedure in Sectie 12. IT Building zal binnen de wettelijke termijnen (in principe uiterlijk binnen één maand) inhoudelijk op jouw verzoek reageren. Houd er rekening mee dat we je om een identiteitsverificatie kunnen vragen voordat we gehoor geven aan je verzoek, om te voorkomen dat onbevoegden toegang krijgen tot jouw gegevens.

11. Vragen en contact

Voor vragen, zorgen of verzoeken met betrekking tot dit privacybeleid of de verwerking van jouw persoonsgegevens kun je contact opnemen met IT Building. In het bijzonder kun je:

- Vragen over of inzage in jouw persoonsgegevens, of verzoeken tot rectificatie, verwijdering, beperking, dataportabiliteit of bezwaar kenbaar maken.
- Meldingen doen als je vermoedt dat er iets misgaat met de bescherming van persoonsgegevens binnen IT Building (bijvoorbeeld een mogelijk datalek, zie ook “Reporting” binnen ons ISMS beleid).

Contactinformatie: Je kunt je in eerste instantie wenden tot de afdeling HR via hr@ITBuilding.nl. Zij zullen je vraag of verzoek behandelen of – waar nodig – doorgeleiden naar de verantwoordelijke functionaris.

Daarnaast kun je ook rechtstreeks contact opnemen met onze Functionaris Gegevensbescherming (FG) voor privacygerelateerde vragen of klachten. De FG is bereikbaar via het e-mailadres privacy@ITBuilding.nl (of alternatieve contactinformatie die intern gecommuniceerd is).

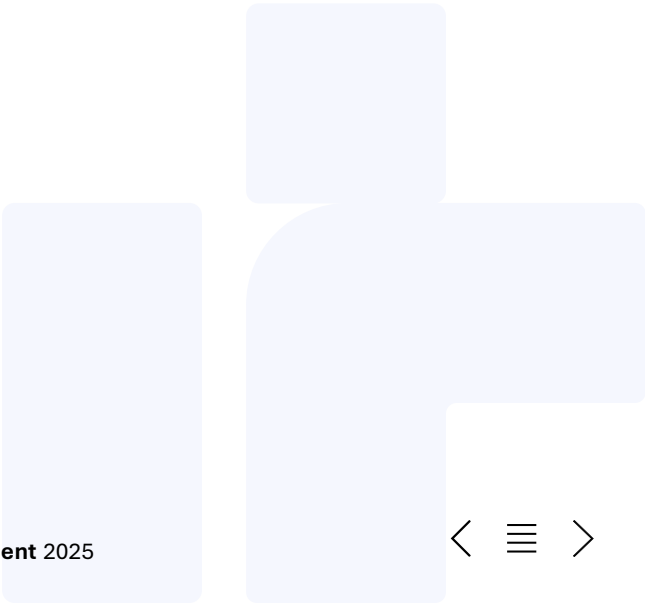
We moedigen medewerkers aan om bij enige onzekerheid of zorgen over privacy tijdig aan de bel te trekken. IT Building streeft ernaar een open cultuur te hanteren rondom privacy, waarbij transparant en constructief met vragen en incidenten wordt omgegaan. Vanzelfsprekend kun je je ook wenden tot de externe toezichthouder (Autoriteit Persoonsgegevens) met klachten, maar we hopen eventuele issues in onderling overleg op te lossen.

12. Wijzigingen

IT Building behoudt zich het recht voor dit interne privacybeleid te wijzigen of te actualiseren. De meest recente versie van het beleid is altijd beschikbaar (bijvoorbeeld in ons ISMS of op het intranet) en vervangt voorgaande versies. We raden je aan om het privacybeleid periodiek te raadplegen, zodat je op de hoogte blijft van eventuele aanpassingen. Bij ingrijpende wijzigingen zal IT Building dit duidelijk aan alle medewerkers communiceren.

Dit beleid is vastgesteld op 24-10-2025 en treedt per direct in werking. Eventuele eerdere interne privacybeleid-documenten komen hiermee te vervallen.

Versie	Datum	Wijziging	Auteur
0.1	01-06-2022	Initiatie	Jimmy de Vos
0.9	01-03-2023	Concept	Debby Markies
1.0	12-05-2023	Definitieve versie	Jimmy de Vos
1.1	28-05-2024	Jaarlijkse review	Suzan Koopman
1.2	29-12-2025	Inhoudelijk herzien	Ryan van Dam



Please note.

(Vermoeden van) datalek of privacy-incident? Meld dit onmiddellijk bij je leidinggevende en HR. Volg de incidentprocedure zoals beschreven in het ISMS. Hierdoor kunnen we tijdig beoordelen en – indien nodig – melden bij de Autoriteit Persoonsgegevens.