

Privacybeleid Lopital Nederland B.V.



Lopital Nederland B.V.
Laarakkenweg 9, 5061 JR Oisterwijk
Tel +31 (0)13 52.39.300, E-mail info@lopital.nl, www.lopital.nl



Lopital België B.V.
Antwerpsesteenweg 124, B-2630 Aartselaar
Tel +32 (0)3 870.51.60, E-mail info@lopital.be, www.lopital.be

IBAN: NL50 INGB 0676 0858 22
BIC: INGBNL2A

BTW/Tax: NL005517692.B01
BTW/Tax: BE0896.717.884
KVK: 18023784

Inhoudsopgave

	Details	3
1.	Inleiding	4
1.1	Geldigheidsduur	4
1.2	Begripsbepalingen	4
1.3	Visie	4
1.4	Doel	4
1.5	Verantwoordelijkheid van medewerkers	4
1.6	Reikwijdte	4
1.7	Verantwoordelijke	4
2.	Principes voor de verwerking van persoonsgegevens	5
2.1	Rechtmatige grondslag	5
2.2	Duidelijke doeleinden	5
2.3	Beperking van verdere verwerking	5
2.4	Minimale gegevensverwerking	5
2.5	Juiste en actuele gegevens	5
2.6	Bewaartermijnen	5
2.7	Integriteit en vertrouwelijkheid	5
2.8	Privacy by Design & Default	5
2.9	Toegang tot gegevens	5
2.10	Inbreuken op persoonsgegevens	6
2.11	Externe verwerkers	6
2.12	Transparantie	6
2.13	Essentiële documentatie	6
2.14	Toezicht en advies	6
3.	Welke persoonsgegevens verwerken wij?	6
4.	Doeleinden van verwerking	7
5.	Rechtsgrondslag voor verwerking	7
6.	Bewaartermijnen	7
7.	Delen van persoonsgegevens met derden	8
7.1	Doorgifte van persoonsgegevens buiten de EU	8
8.	Beveiligingsmaatregelen	8
9.	Rechten van betrokkenen	9
9.1.	Regels voor medewerkers	9

10.	Interne procedures bij Lopital.....	9
11.	Rollen en verantwoordelijken	10
12.	Wijzigingen in dit beleid	10

Details

Documenthistorie

Uitgegeven door: Iris Brans
Vrijgegeven door: Iris Brans
Datum: 28-3-2025
Status: Concept
Versie: 1.0

Versiebeheer

Datum	Naam	Wijziging	Versie
28-03-2025	Iris Brans	Opzet document	1.0

1. Inleiding

Lopital Nederland B.V. (hierna: Lopital) verwerkt persoonsgegevens van medewerkers om een veilige, efficiënte en professionele werkomgeving te waarborgen. Dit privacybeleid beschrijft hoe Lopital omgaat met de persoonsgegevens van medewerkers en hoe wordt voldaan aan de Algemene Verordening Gegevensbescherming (AVG).

1.1 Geldigheidsduur

Dit beleid is vastgesteld door de directie van Lopital in samenwerking met een Adviseur Cybersecurity en Informatiebeveiliging. Het wordt minimaal eens per jaar geëvalueerd en indien nodig geactualiseerd.

1.2 Begripsbepalingen

De definities uit artikel 4 van de AVG zijn van toepassing op dit privacybeleid.

1.3 Visie

Lopital streeft naar een sterke privacy cultuur, waarin medewerkers zich bewust zijn van het belang van gegevensbescherming. Verantwoord omgaan met persoonsgegevens is essentieel voor een veilige werkomgeving en draagt bij aan de bescherming van medewerkersrechten. Privacy is een gezamenlijke verantwoordelijkheid binnen de organisatie.

1.4 Doel

Dit beleid biedt een kader voor de zorgvuldige verwerking van persoonsgegevens van medewerkers en legt verantwoordelijkheden op het gebied van gegevensbescherming vast. De praktische uitvoering van dit beleid wordt verder uitgewerkt in interne richtlijnen en procedures, zoals:

- Datalekprocedure conform artikel 33 AVG.
- Privacy by Design & Default bij interne systemen en processen.
- Toegangs- en beveiligingsbeleid voor IT-systemen en fysieke documenten.

Lopital hanteert daarnaast een cyberhygiënebeleid en een cybersecuritybeleid om de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens te waarborgen.

1.5 Verantwoordelijkheid van medewerkers

Elke medewerker is verantwoordelijk voor de naleving van dit beleid en het zorgvuldig omgaan met persoonsgegevens. Lopital verwacht dat medewerkers privacyregels volgen en bijdragen aan een privacy bewuste werkomgeving.

1.6 Reikwijdte

Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens binnen Lopital met betrekking tot medewerkers, waaronder:

1. Personeelsadministratie, zoals loonverwerking en verlofregistratie.
2. IT- en toegangsbeheer, inclusief e-mailgebruik en werkplekmonitoring.
3. Gegevensuitwisseling met externe dienstverleners, zoals salarisverwerkers en arbodiensten.

Lopital verwerkt uitsluitend persoonsgegevens van medewerkers voor legitieme en noodzakelijke doeleinden en committeert zich aan een transparante en veilige verwerking zoals gesteld in Artikel 5 en artikel 13 van de AVG.

1.7 Verantwoordelijke

Lopital is de verwerkingsverantwoordelijke voor de persoonsgegevens van medewerkers. Vragen over dit beleid kunnen worden gesteld aan de Manager Finance.

2. Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. Lopital onderschrijft deze principes en verwerkt persoonsgegevens van medewerkers uitsluitend in overeenstemming met deze uitgangspunten.

2.1 Rechtmatige grondslag

Lopital verwerkt persoonsgegevens van medewerkers uitsluitend in overeenstemming met de wet en op een zorgvuldige manier. Dit betekent dat gegevensverwerking alleen plaatsvindt als hiervoor een rechtmatige grondslag bestaat, zoals de uitvoering van de arbeidsovereenkomst, een wettelijke verplichting of een gerechtvaardigd belang van Lopital.

2.2 Duidelijke doeleinden

Persoonsgegevens van medewerkers worden uitsluitend verwerkt voor vooraf bepaalde en gerechtvaardigde doeleinden, zoals salarisadministratie, personeelsbeheer, verzuimregistratie en beveiliging. Er worden geen persoonsgegevens verwerkt die niet noodzakelijk zijn voor deze doelen.

2.3 Beperking van verdere verwerking

Persoonsgegevens van medewerkers worden alleen voor andere doeleinden gebruikt als deze verenigbaar zijn met het oorspronkelijke doel, er geen nadelige gevolgen voor de medewerker zijn en er aanvullende waarborgen zijn getroffen.

2.4 Minimale gegevensverwerking

Lopital verwerkt alleen die persoonsgegevens die strikt noodzakelijk zijn voor het betreffende doel. Indien mogelijk, wordt gekozen voor een verwerking met minder gegevens of pseudonimisering.

2.5 Juiste en actuele gegevens

Lopital zorgt ervoor dat de persoonsgegevens van medewerkers correct en actueel zijn. Medewerkers worden aangemoedigd om wijzigingen in hun gegevens tijdig door te geven. Onjuiste of verouderde gegevens worden zo snel mogelijk aangepast of verwijderd.

2.6 Bewaartermijnen

Persoonsgegevens van medewerkers worden niet langer bewaard dan noodzakelijk voor het doel waarvoor ze zijn verzameld of zolang als wettelijk vereist. Na afloop van de bewaartermijn worden gegevens verwijderd of geanonimiseerd. Meer informatie hierover is te vinden in Hoofdstuk 6.

2.7 Integriteit en vertrouwelijkheid

Lopital neemt technische en organisatorische maatregelen om persoonsgegevens van medewerkers te beschermen tegen verlies, ongeautoriseerde toegang of onrechtmatige verwerking. Dit beleid sluit aan op het interne cyberhygiëne- en cybersecuritybeleid.

2.8 Privacy by Design & Default

Bij de invoering van nieuwe systemen of processen wordt privacy vanaf het ontwerp meegenomen, zodat persoonsgegevens optimaal beschermd zijn. Standaardinstellingen worden zo privacy vriendelijk mogelijk ingericht.

2.9 Toegang tot gegevens

Uitsluitend geautoriseerde medewerkers hebben toegang tot personeelsgegevens. Toegangsrechten worden periodiek geëvalueerd en vastgelegd in het toegangsbeleid binnen het cybersecuritybeleid. Ongeautoriseerde toegang wordt actief voorkomen.

2.10 Inbreuken op persoonsgegevens

Bij een datalek of ongeoorloofde toegang tot persoonsgegevens wordt gehandeld conform de interne procedure voor datalekken. Indien nodig wordt er een melding gemaakt bij de Autoriteit Persoonsgegevens en worden betrokken medewerkers geïnformeerd.

2.11 Externe verwerkers

Wanneer Lopital externe partijen inschakelt voor het verwerken van medewerkersgegevens (bijvoorbeeld salarisadministratie), worden hiervoor contractuele afspraken vastgelegd in verwerkersovereenkomsten. Externe partijen moeten een passend niveau van gegevensbescherming waarborgen.

2.12 Transparantie

Medewerkers worden duidelijk geïnformeerd over hoe Lopital hun persoonsgegevens verwerkt en welke rechten zij hebben. Dit gebeurt via dit privacybeleid en aanvullende informatie in het personeelshandboek of via interne communicatiekanalen.

2.13 Essentiële documentatie

Om te voldoen aan de AVG en privacybescherming te waarborgen, beschikt Lopital over de volgende documentatie:

- Verwerkingsregister met personeelsgegevens;
- Verwerkersovereenkomsten met externe partijen;
- Intern privacybeleid voor medewerkers;
- Cybersecurity Risk Assessment;
- Cyberhygiënebeleid;
- Cybersecuritybeleid;
- Datalekregister en -protocol.

2.14 Toezicht en advies

Lopital heeft geen wettelijke verplichting om een Functionaris Gegevensbescherming (FG) aan te stellen. Wel wordt waar nodig een extern adviseur ingeschakeld voor advies over informatiebeveiliging en privacy. Intern houdt de Manager Finance toezicht op naleving van dit beleid.

3. Welke persoonsgegevens verwerken wij?

Lopital verwerkt persoonsgegevens van (potentiële) medewerkers en voormalige medewerkers. Wij verwerken onder andere de volgende persoonsgegevens:

- Identificatiegegevens (zoals naam, geboortedatum, BSN, kopie ID);
- Contactgegevens (adres, telefoonnummer, e-mailadres);
- Financiële gegevens (bankrekeningnummer, salarisgegevens, loonheffingen);
- Verlof- en verzuimgegevens (registratie van afwezigheid, re-integratiedossiers);
- Arbeid gerelateerde gegevens (functie, contractgegevens, prestaties, beoordelingen, opleidingsgegevens);
- Sollicitatiegegevens (CV, motivatiebrief en andere informatie verstrekt tijdens een sollicitatieprocedure);
- Overige gegevens die medewerkers actief verstrekken, bijvoorbeeld in correspondentie of telefonisch.

4. Doeleinden van verwerking

Lopital verwerkt persoonsgegevens van medewerkers uitsluitend voor de volgende doeleinden:

- Het aangaan, uitvoeren en beëindigen van arbeidsovereenkomsten en andere werkrelaties;
- Het voeren van de personeelsadministratie, salarisadministratie en verzuimregistratie;
- Het voldoen aan wettelijke verplichtingen (zoals belastingwetgeving, sociale zekerheidswetgeving en Arbowetgeving);
- Het waarborgen van een veilige en efficiënte werkomgeving (bijv. toegangsbeheer, IT-beveiliging);
- Het beheren van personeelsdossiers en het beoordelen van prestaties en ontwikkeling;
- Het faciliteren van opleidingen, trainingen en ontwikkelingsprogramma's;
- Het registreren van verlof en verzuim;
- Het onderhouden van communicatie met medewerkers over bedrijf gerelateerde onderwerpen;
- Het behandelen van klachten, geschillen of juridische procedures waarin medewerkers betrokken zijn;
- Archiefdoeleinden, waarbij gegevens uitsluitend worden gebruikt bij juridische procedures of voor historische, statistische of wetenschappelijke doeleinden.

Lopital verwerkt persoonsgegevens via onder andere de HR-afdeling, salarisadministratie en IT-systemen. Dit gebeurt op basis van wettelijke verplichtingen, de uitvoering van de arbeidsovereenkomst of het gerechtvaardigd belang van Lopital. Gegevens worden uitsluitend verwerkt voor het betreffende doel en niet zonder voorafgaande toestemming voor andere doeleinden gebruikt.

In sommige gevallen kunnen gegevens, in geanonimiseerde vorm, worden gebruikt voor statistische analyses en rapportages.

5. Rechtsgrondslag voor verwerking

Wij verwerken persoonsgegevens op basis van:

- Toestemming van de betrokkene (Artikel 6 lid 1 sub a AVG);
- Uitvoering van een overeenkomst (Artikel 6 lid 1 sub b AVG);
- Wettelijke verplichting (Artikel 6 lid 1 sub c AVG);
- Gerechtvaardigd belang (Artikel 6 lid 1 sub f AVG).

Lopital verwerkt bepaalde persoonsgegevens van medewerkers op basis van gerechtvaardigd belang (Artikel 6 lid 1 sub f AVG). Dit houdt in dat de verwerking noodzakelijk is voor een legitiem doel van Lopital, mits dit belang zwaarder weegt dan de privacyrechten van medewerkers.

Voorbeelden van gerechtvaardigde belangen:

- IT- en bedrijfsbeveiliging: Toegangscontrole, netwerkmonitoring en fraudepreventie.
- Efficiënte bedrijfsvoering: Personeelsadministratie, interne communicatie en roosterbeheer.
- Prestatiebeheer en kwaliteitscontrole: Functioneringsgesprekken en het afhandelen van klachten.

Lopital weegt bij elke verwerking af of deze noodzakelijk en proportioneel is en neemt passende maatregelen om privacy risico's te minimaliseren. Medewerkers kunnen bezwaar maken als zij vinden dat hun privacybelang zwaarder weegt.

6. Bewaartermijnen

Wij bewaren persoonsgegevens niet langer dan noodzakelijk voor het doel waarvoor ze zijn verzameld, tenzij een langere bewaartermijn wettelijk vereist is. De volgende bewaartermijnen worden gehanteerd:

Type persoonsgegevens	Bewaartermijn	Wettelijke basis / reden
Identificatiegegevens	5 jaar na uitdiensttreding	Fiscaal en sociaal zekerheidsrecht
Contactgegevens	Tot 2 jaar na uitdiensttreding	Alleen indien nodig voor referentie
Financiële gegevens	7 jaar na uitdiensttreding	Belastingwetgeving
Verlof- en verzuimgegevens	2 jaar na herstel	Wet verbetering Poortwachter
Arbeidscontract en gerelateerde documenten	7 jaar na einde dienstverband	Fiscale en arbeidsrechtelijke verplichtingen
Beoordelingen en functioneringsgesprekken	Tot 2 jaar na uitdiensttreding	Best practice, tenzij juridisch relevant
Sollicitatiegegevens	4 weken na afwijzing (of 1 jaar met toestemming)	AVG-richtlijnen
Opleidings- en trainingsgegevens	Tot 2 jaar na uitdiensttreding	Relevantie voor HR-administratie

7. Delen van persoonsgegevens met derden

Tenzij in dit beleid anders vermeld, worden persoonsgegevens van medewerkers niet verhuurd, verkocht of op andere wijze gedeeld met derden. Lopital kan gegevens met derden delen wanneer de medewerker hier expliciet toestemming voor heeft gegeven of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting, zoals een verzoek van handhavende autoriteiten of fraude bestrijdende organisaties.

Daarnaast kunnen zakelijke dienstverleners in opdracht van Lopital bepaalde HR- of administratieve processen uitvoeren, zoals salarisadministratie of IT-dienstverlening. Met deze verwerkers worden contractuele afspraken gemaakt om een vertrouwelijke en zorgvuldige omgang met persoonsgegevens te waarborgen, vastgelegd in verwerkersovereenkomsten.

7.1 Doorgifte van persoonsgegevens buiten de EU

Lopital verstrekt in principe geen persoonsgegevens van medewerkers aan landen buiten de EU. Mocht dit toch noodzakelijk zijn voor bijvoorbeeld IT-diensten of salarisverwerking, dan gebeurt dit alleen met passende waarborgen, zoals:

- Een adequaatheidsbesluit van de Europese Commissie, indien van toepassing.
- Modelcontracten goedgekeurd door de Europese Commissie die de bescherming van persoonsgegevens garanderen.
- Expliciete toestemming van de medewerker in specifieke gevallen.

Lopital neemt maatregelen om de veiligheid en vertrouwelijkheid van gegevens bij internationale doorgifte te waarborgen.

8. Beveiligingsmaatregelen

Wij nemen passende technische en organisatorische maatregelen om persoonsgegevens te beschermen, waaronder:

- Beveiligde opslag en versleuteling van gegevens;
- Toegangscontrole en autorisatiebeheer;
- Periodieke audits en updates;
- Beleid voor incidentmanagement en datalekken;
- Multifactor authenticatie voor kritieke accounts of systemen;
- Regelmatige back-ups;
- Rol gebaseerde toegang;
- SSL beveiliging;
- Wachtwoordbeveiliging en beleid;
- Firewall;

- Logging;
- Netwerksegmentatie;
- Virus, malware en phishing detectie;
- Automatische updates en patches;
- Benodigde organisatorische documentatie;
- Datalek protocol en register;
- Cybersecurity Risk Assessment.

9. Rechten van betrokkenen

Betrokkenen hebben de volgende rechten:

1. Recht op inzage – Artikel 15 AVG

Betrokkenen hebben het recht om te weten welke persoonsgegevens van hen worden verwerkt en voor welke doeleinden.

2. Recht op vergetelheid (recht op verwijdering) – Artikel 17 AVG

Betrokkenen kunnen verzoeken om hun persoonsgegevens te laten verwijderen, mits er geen wettelijke verplichting is om deze te bewaren.

3. Recht op rectificatie of aanvulling – Artikel 16 AVG

Betrokkenen kunnen onjuiste of onvolledige gegevens laten corrigeren of aanvullen.

4. Recht op data portabiliteit – Artikel 20 AVG

Betrokkenen hebben het recht om hun persoonsgegevens in een gestructureerd, gangbaar en machine leesbaar formaat te ontvangen en deze door te geven aan een andere organisatie.

5. Recht om toestemming in te trekken – Artikel 7 lid 3 AVG

Wanneer verwerking is gebaseerd op toestemming, heeft de betrokkene het recht om deze toestemming op elk moment in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van eerdere verwerking.

6. Recht op beperking van verwerking – Artikel 18 AVG

Betrokkenen kunnen onder bepaalde omstandigheden verzoeken om de verwerking van hun persoonsgegevens tijdelijk te beperken, bijvoorbeeld als de juistheid van de gegevens wordt betwist.

7. Recht op bezwaar – Artikel 21 AVG

Betrokkenen kunnen bezwaar maken tegen de verwerking van hun persoonsgegevens op basis van gerechtvaardigd belang of voor direct marketingdoeleinden.

9.1 Regels voor medewerkers

De regels voor medewerkers zijn beschreven in het cyberhygiënebeleid.

10. Interne procedures bij Lopital

Binnen Lopital zijn er onder andere de volgende interne procedures om de cybersecurity en informatiebeveiliging te borgen:

- **Privacy-audit:** AMVM Advies voert een interne privacy-audit uit.
- **Datalekprocedure:** Datalekken worden binnen 72 uur gemeld aan de Autoriteit Persoonsgegevens conform Artikel 33 AVG.
- **Privacy by Design & Default:** Alle systemen en processen worden zo ontworpen dat privacybescherming gewaarborgd is (Artikel 25 AVG).

- **Incidentenbeheer:** Een protocol voor het identificeren en aanpakken van beveiligingsincidenten is beschikbaar voor alle medewerkers.
- **Verwerkingsregister:** Lopital houdt een register bij van alle gegevensverwerkingsactiviteiten (Artikel 30 AVG).
- **Risicoanalyse en beheer:** Lopital heeft een risicoanalyse gericht op interne processen, systemen, gegevens en andere IT & OT middelen. N.a.v. deze risicoanalyse worden er beheersmaatregelen getroffen om de risico's geprioriteerd en gemitigeerd.

11. Rollen en verantwoordelijken

Binnen Lopital zijn er rollen en verantwoordelijken met betrekking tot de AVG en algehele cybersecurity. Hieronder is een overzicht beschreven.

- **Directeur:** Eindverantwoordelijk voor naleving AVG.
- **Manager Finance:** Verantwoordelijk voor interne communicatie, naleving van beleid en procedures.
- **AMVM Advies:** Verantwoordelijk voor het adviseren en ondersteunen met betrekking tot privacy en cybersecurity waar nodig.
- **Algemene medewerker:** Verantwoordelijk voor het adequaat werken met persoonsgegevens en naleven van beleid.

12. Wijzigingen in dit beleid

Dit privacybeleid kan worden gewijzigd. De meest actuele versie is altijd beschikbaar. Belangrijke wijzigingen worden actief gecommuniceerd door de Manager Finance.