

Datenschutzerklärung Lopital Nederland B.V.



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

IBAN: NL50 INGB 0676 0858 22
BIC: INGBNL2A

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



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

Inhaltsverzeichnis

Einzelheiten	3
1. Einleitung	4
1.1 Gültigkeitsdauer.....	4
1.2 Begriffsbestimmungen.....	4
1.3 Vision.....	4
1.4 Zweck.....	4
1.5 Verantwortung der Mitarbeiter.....	4
1.6 Geltungsbereich.....	4
1.7 Verantwortlicher.....	4
2. Grundsätze für die Verarbeitung personenbezogener Daten	5
2.1 Rechtmäßige Grundlage.....	5
2.2 Klare Zwecke.....	5
2.3 Beschränkung der Weiterverarbeitung.....	5
2.4 Minimale Datenverarbeitung.....	5
2.5 Korrekte und aktuelle Daten.....	5
2.6 Aufbewahrungsfristen.....	5
2.7 Integrität und Vertraulichkeit.....	5
2.8 Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen.....	5
2.9 Zugriff auf Daten.....	5
2.10 Verstöße gegen den Datenschutz.....	6
2.11 Externe Verarbeiter.....	6
2.12 Transparenz.....	6
2.13 Wesentliche Dokumentation.....	6
2.14 Aufsicht und Beratung.....	6
3. Welche personenbezogenen Daten verarbeiten wir?	6
4. Zweck der Verarbeitung	7
5. Rechtsgrundlage für die Verarbeitung	7
6. Aufbewahrungsfristen	7
7. Weitergabe personenbezogener Daten an Dritte	8
7.1 Übermittlung personenbezogener Daten außerhalb der EU.....	8
8. Sicherheitsmaßnahmen	8
9. Rechte der betroffenen Personen	9
9.1 Regeln für Mitarbeiter.....	9

10.	Interne Verfahren bei Lopital	10
11.	Rollen und Verantwortlichkeiten	10
12.	Änderungen dieser Richtlinie	10

Einzelheiten

Dokumenthistorie

Herausgegeben von: Iris Brans
Freigegeben von: Iris Brans
Datum: 28-3-2025
Status: Entwurf
Version: 1.0

Version Verwaltung

Datum	Name	Änderung	Version
28-03-2025	Iris Brans	Aufbau des Dokuments	1.0

1. Einleitung

Lopital Nederland B.V. (im Folgenden: Lopital) verarbeitet personenbezogene Daten von Mitarbeitern, um ein sicheres, effizientes und professionelles Arbeitsumfeld zu gewährleisten. Diese Datenschutzerklärung beschreibt, wie Lopital mit den personenbezogenen Daten von Mitarbeitern umgeht und wie die Datenschutz-Grundverordnung (DSGVO) eingehalten wird).

1.1 Gültigkeitsdauer

Diese Richtlinie wurde von der Geschäftsführung von Lopital in Zusammenarbeit mit einem Berater für Cybersicherheit und Informationssicherheit festgelegt. Sie wird mindestens einmal jährlich überprüft und bei Bedarf aktualisiert.

1.2 Begriffsbestimmungen

Die Definitionen in Artikel 4 der DSGVO gelten für diese Datenschutzerklärung.

1.3 Vision

Lopital strebt eine starke Datenschutzkultur an, in der sich die Mitarbeiter der Bedeutung des Datenschutzes bewusst sind. Der verantwortungsvolle Umgang mit personenbezogenen Daten ist für ein sicheres Arbeitsumfeld unerlässlich und trägt zum Schutz der Rechte der Mitarbeiter bei. Datenschutz ist eine gemeinsame Verantwortung innerhalb der Organisation.

1.4 Zweck

Diese Richtlinie bietet einen Rahmen für die sorgfältige Verarbeitung personenbezogener Daten von Mitarbeitern und legt Verantwortlichkeiten im Bereich des Datenschutzes fest. Die praktische Umsetzung dieser Richtlinie wird in internen Richtlinien und Verfahren näher ausgeführt, wie zum Beispiel:

- Verfahren bei Datenschutzverletzungen gemäß Artikel 33 der DSGVO.
- Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen bei internen Systemen und Prozessen.
- Zugangs- und Sicherheitsrichtlinien für IT-Systeme und physische Dokumente.

Darüber hinaus verfügt Lopital über eine Cyberhygiene-Richtlinie und eine Cybersicherheitsrichtlinie, um die Verfügbarkeit, Integrität und Vertraulichkeit personenbezogener Daten zu gewährleisten.

1.5 Verantwortung der Mitarbeiter

Jeder Mitarbeiter ist für die Einhaltung dieser Richtlinie und den sorgfältigen Umgang mit personenbezogenen Daten verantwortlich. Lopital erwartet von seinen Mitarbeitern, dass sie die Datenschutzbestimmungen einhalten und zu einer datenschutzbewussten Arbeitsumgebung beitragen.

1.6 Geltungsbereich

Diese Richtlinie gilt für alle Verarbeitungen personenbezogener Daten innerhalb von Lopital in Bezug auf Mitarbeiter, darunter:

1. Personalverwaltung, wie Lohnabrechnung und Urlaubsregistrierung.
2. IT- und Zugangsverwaltung, einschließlich E-Mail-Nutzung und Arbeitsplatzüberwachung.
3. Datenaustausch mit externen Dienstleistern, wie Lohnbuchhaltern und Arbeitsschutzdiensten.

Lopital verarbeitet personenbezogene Daten von Mitarbeitern ausschließlich für legitime und notwendige Zwecke und verpflichtet sich zu einer transparenten und sicheren Verarbeitung gemäß Artikel 5 und Artikel 13 der DSGVO.

1.7 Verantwortlicher

Lopital ist der Verantwortliche für die Verarbeitung personenbezogener Daten von Mitarbeitern. Fragen zu dieser Richtlinie können an den Finanzmanager gerichtet werden.

2. Grundsätze für die Verarbeitung personenbezogener Daten

Die DSGVO basiert auf einer Reihe von Grundsätzen für die Verarbeitung personenbezogener Daten. Lopital bekennt sich zu diesen Grundsätzen und verarbeitet personenbezogene Daten von Mitarbeitern ausschließlich in Übereinstimmung mit diesen Grundsätzen.

2.1 Rechtmäßige Grundlage

Lopital verarbeitet personenbezogene Daten von Mitarbeitern ausschließlich in Übereinstimmung mit den gesetzlichen Bestimmungen und mit der gebotenen Sorgfalt. Dies bedeutet, dass eine Datenverarbeitung nur dann erfolgt, wenn dafür eine rechtmäßige Grundlage besteht, wie beispielsweise die Erfüllung des Arbeitsvertrags, eine gesetzliche Verpflichtung oder ein berechtigtes Interesse von Lopital.

2.2 Klare Zwecke

Personenbezogene Daten von Mitarbeitern werden ausschließlich für zuvor festgelegte und berechtigte Zwecke verarbeitet, wie beispielsweise Lohnbuchhaltung, Personalverwaltung, Abwesenheitserfassung und Sicherheit. Es werden keine personenbezogenen Daten verarbeitet, die für diese Zwecke nicht erforderlich sind.

2.3 Beschränkung der Weiterverarbeitung

Personenbezogene Daten von Mitarbeitern werden nur dann für andere Zwecke verwendet, wenn diese mit dem ursprünglichen Zweck vereinbar sind, keine nachteiligen Auswirkungen auf den Mitarbeiter haben und zusätzliche Garantien getroffen wurden.

2.4 Minimale Datenverarbeitung

Lopital verarbeitet nur personenbezogene Daten, die für den jeweiligen Zweck unbedingt erforderlich sind. Wenn möglich, wird eine Verarbeitung mit weniger Daten oder eine Pseudonymisierung gewählt.

2.5 Korrekte und aktuelle Daten

Lopital sorgt dafür, dass die personenbezogenen Daten der Mitarbeiter korrekt und aktuell sind. Die Mitarbeiter werden dazu angehalten, Änderungen ihrer Daten rechtzeitig mitzuteilen. Falsche oder veraltete Daten werden so schnell wie möglich angepasst oder gelöscht.

2.6 Aufbewahrungsfristen

Personenbezogene Daten von Mitarbeitern werden nicht länger gespeichert, als es für den Zweck, für den sie erhoben wurden, erforderlich ist oder solange es gesetzlich vorgeschrieben ist. Nach Ablauf der Aufbewahrungsfrist werden die Daten gelöscht oder anonymisiert. Weitere Informationen hierzu finden Sie in Kapitel 6.

2.7 Integrität und Vertraulichkeit

Lopital ergreift technische und organisatorische Maßnahmen, um personenbezogene Daten von Mitarbeitern vor Verlust, unbefugtem Zugriff oder unrechtmäßiger Verarbeitung zu schützen. Diese Richtlinie steht im Einklang mit den internen Richtlinien zur Cyberhygiene und Cybersicherheit.

2.8 Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen

Bei der Einführung neuer Systeme oder Prozesse wird der Datenschutz bereits in der Entwurfsphase berücksichtigt, um einen optimalen Schutz personenbezogener Daten zu gewährleisten. Die Standardeinstellungen werden so datenschutzfreundlich wie möglich gestaltet.

2.9 Zugriff auf Daten

Nur autorisierte Mitarbeiter haben Zugriff auf Personaldaten. Zugriffsrechte werden regelmäßig überprüft und in der Zugriffsrichtlinie innerhalb der Cybersicherheitsrichtlinie festgelegt. Unbefugter Zugriff wird aktiv verhindert.

2.10 Verstöße gegen den Datenschutz

Bei einer Datenpanne oder einem unbefugten Zugriff auf personenbezogene Daten wird gemäß dem internen Verfahren für Datenpannen vorgegangen. Falls erforderlich, wird eine Meldung an die Datenschutzbehörde gemacht und die betroffenen Mitarbeiter werden informiert.

2.11 Externe Verarbeiter

Wenn Lopital externe Parteien mit der Verarbeitung von Mitarbeiterdaten beauftragt (z. B. Lohnbuchhaltung), werden hierfür vertragliche Vereinbarungen in Verarbeitungsverträgen festgelegt. Externe Parteien müssen ein angemessenes Datenschutzniveau gewährleisten.

2.12 Transparenz

Die Mitarbeiter werden klar darüber informiert, wie Lopital ihre personenbezogenen Daten verarbeitet und welche Rechte sie haben. Dies geschieht über diese Datenschutzerklärung und zusätzliche Informationen im Personalhandbuch oder über interne Kommunikationskanäle.

2.13 Wesentliche Dokumentation

Um die DSGVO einzuhalten und den Datenschutz zu gewährleisten, verfügt Lopital über die folgende Dokumentation:

- Verarbeitungsverzeichnis mit Personaldaten;
- Verarbeitungsvereinbarungen mit externen Parteien;
- Interne Datenschutzrichtlinie für Mitarbeiter;
- Cybersicherheits-Risikobewertung;
- Cyberhygiene-Richtlinie;
- Cybersicherheitsrichtlinie;
- Datenverarbeitungsregister und -protokoll.

2.14 Aufsicht und Beratung

Lopital ist gesetzlich nicht verpflichtet, einen Datenschutzbeauftragten zu ernennen. Bei Bedarf wird jedoch ein externer Berater hinzugezogen, der in Fragen der Informationssicherheit und des Datenschutzes berät. Intern überwacht der Finanzmanager die Einhaltung dieser Richtlinie.

3. Welche personenbezogenen Daten verarbeiten wir?

Lopital verarbeitet personenbezogene Daten von (potenziellen) Mitarbeitern und ehemaligen Mitarbeitern. Wir verarbeiten unter anderem die folgenden personenbezogenen Daten:

- Identifikationsdaten (wie Name, Geburtsdatum, Sozialversicherungsnummer, Kopie des Personalausweises);
- Kontaktdaten (Adresse, Telefonnummer, E-Mail-Adresse);
- Finanzdaten (Bankverbindung, Gehaltsdaten, Lohnabgaben);
- Urlaubs- und Abwesenheitsdaten (Erfassung von Abwesenheiten, Wiedereingliederungsunterlagen);
- Arbeitsbezogene Daten (Funktion, Vertragsdaten, Leistungen, Beurteilungen, Ausbildungsdaten);
- Bewerbungsdaten (Lebenslauf, Motivationsschreiben und andere im Rahmen eines Bewerbungsverfahrens bereitgestellte Informationen);
- Sonstige Daten, die Mitarbeiter aktiv bereitstellen, beispielsweise in der Korrespondenz oder telefonisch.

4. Zweck der Verarbeitung

Lopital verarbeitet personenbezogene Daten von Mitarbeitern ausschließlich für die folgenden Zwecke:

- Abschluss, Durchführung und Beendigung von Arbeitsverträgen und anderen Arbeitsverhältnissen;
- Personalverwaltung, Lohnbuchhaltung und Abwesenheitserfassung;
- Erfüllung gesetzlicher Verpflichtungen (z. B. Steuerrecht, Sozialversicherungsrecht und Arbeitsschutzrecht);
- Gewährleistung einer sicheren und effizienten Arbeitsumgebung (z. B. Zugangskontrolle, IT-Sicherheit);
- Verwaltung von Personalakten und Beurteilung von Leistungen und Entwicklungen;
- Bereitstellung von Schulungen, Fortbildungen und Entwicklungsprogrammen;
- Erfassung von Urlaub und Abwesenheiten;
- Kommunikation mit Mitarbeitern zu unternehmensbezogenen Themen;
- Bearbeitung von Beschwerden, Streitigkeiten oder Gerichtsverfahren, an denen Mitarbeiter beteiligt sind;
- Archivierungszwecke, wobei Daten ausschließlich für Gerichtsverfahren oder für historische, statistische oder wissenschaftliche Zwecke verwendet werden.

Lopital verarbeitet personenbezogene Daten unter anderem über die Personalabteilung, die Lohnbuchhaltung und IT-Systeme. Dies geschieht auf der Grundlage gesetzlicher Verpflichtungen, der Erfüllung des Arbeitsvertrags oder des berechtigten Interesses von Lopital. Daten werden ausschließlich für den jeweiligen Zweck verarbeitet und nicht ohne vorherige Zustimmung für andere Zwecke verwendet.

In einigen Fällen können Daten in anonymisierter Form für statistische Analysen und Berichte verwendet werden.

5. Rechtsgrundlage für die Verarbeitung

Wir verarbeiten personenbezogene Daten auf der Grundlage:

- Einwilligung der betroffenen Person (Artikel 6 Absatz 1 Buchstabe a DSGVO);
- Erfüllung eines Vertrags (Artikel 6 Absatz 1 Buchstabe b DSGVO);
- Gesetzliche Verpflichtung (Artikel 6 Absatz 1 Buchstabe c DSGVO);
- Berechtigtes Interesse (Artikel 6 Absatz 1 Buchstabe f DSGVO).

Lopital verarbeitet bestimmte personenbezogene Daten von Mitarbeitern auf der Grundlage eines berechtigten Interesses (Artikel 6 Absatz 1 Buchstabe f DSGVO). Dies bedeutet, dass die Verarbeitung für einen legitimen Zweck von Lopital erforderlich ist, sofern dieses Interesse nicht die Datenschutzrechte der Mitarbeiter überwiegt.

Beispiele für berechnigte Interessenbelangen:

- IT- und Unternehmenssicherheit: Zugangskontrolle, Netzwerküberwachung und Betrugsprävention.
- Effiziente Geschäftsabläufe: Personalverwaltung, interne Kommunikation und Dienstplanverwaltung.
- Leistungsmanagement und Qualitätskontrolle: Mitarbeitergespräche und Bearbeitung von Beschwerden.

Lopital wägt bei jeder Verarbeitung ab, ob diese notwendig und verhältnismäßig ist, und ergreift geeignete Maßnahmen, um Datenschutzrisiken zu minimieren. Mitarbeiter können Widerspruch einlegen, wenn sie der Meinung sind, dass ihr Datenschutzinteresse überwiegt.

6. Aufbewahrungsfristen

Wir bewahren personenbezogene Daten nicht länger auf, als es für den Zweck, für den sie erhoben wurden, erforderlich ist, es sei denn, eine längere Aufbewahrungsfrist ist gesetzlich vorgeschrieben. Es gelten die folgenden Aufbewahrungsfristen:

Art der personenbezogenen Daten	Aufbewahrungsfrist	Rechtsgrundlage / Grund
Identifikationsdaten	5 Jahre nach Ausscheiden aus dem Dienst	Steuer- und Sozialversicherungsrecht
Kontaktdaten	Bis zu 2 Jahre nach Ausscheiden aus dem Dienst	Nur bei Bedarf als Referenz
Finanzdaten	7 Jahre nach Ausscheiden aus dem Dienst	Steuergesetzgebung
Urlaubs- und Abwesenheitsdaten	2 Jahre nach Wiederherstellung	Gesetz zur Verbesserung der Arbeitsvermittlung
Arbeitsvertrag und zugehörige Dokumente	7 Jahre nach Beendigung des Arbeitsverhältnisses	Steuer- und arbeitsrechtliche Verpflichtungen
Beurteilungen und Mitarbeitergespräche	Bis zu 2 Jahre nach Ausscheiden aus dem Dienst	Bewährte Verfahren, sofern nicht rechtlich relevant
Bewerbungsdaten	4 Wochen nach Ablehnung (oder 1 Jahr mit Zustimmung)	DSGVO-Richtlinien
Ausbildungs- und Schulungsdaten	Bis zu 2 Jahre nach Ausscheiden aus dem Dienst	Relevanz für die Personalverwaltung

7. Weitergabe personenbezogener Daten an Dritte

Sofern in dieser Richtlinie nicht anders angegeben, werden personenbezogene Daten von Mitarbeitern nicht an Dritte vermietet, verkauft oder auf andere Weise weitergegeben. Lopital kann Daten an Dritte weitergeben, wenn der Mitarbeiter ausdrücklich seine Zustimmung dazu gegeben hat oder wenn dies zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist, beispielsweise auf Anfrage von Strafverfolgungsbehörden oder Betrugsbekämpfungsorganisationen.

Darüber hinaus können Dienstleister im Auftrag von Lopital bestimmte HR- oder Verwaltungsprozesse durchführen, wie z. B. die Lohnbuchhaltung oder IT-Dienstleistungen. Mit diesen Auftragsverarbeitern werden vertragliche Vereinbarungen getroffen, um einen vertraulichen und sorgfältigen Umgang mit personenbezogenen Daten zu gewährleisten, die in Auftragsverarbeitungsverträgen festgelegt sind.

7.1 Übermittlung personenbezogener Daten außerhalb der EU

Lopital gibt grundsätzlich keine personenbezogenen Daten von Mitarbeitern an Länder außerhalb der EU weiter. Sollte dies dennoch erforderlich sein, beispielsweise für IT-Dienstleistungen oder die Gehaltsabrechnung, erfolgt dies nur mit geeigneten Garantien, wie zum Beispiel:

- Eine Angemessenheitsentscheidung der Europäischen Kommission, sofern zutreffend.
- Von der Europäischen Kommission genehmigte Musterverträge, die den Schutz personenbezogener Daten gewährleisten.
- Ausdrückliche Zustimmung des Mitarbeiters in bestimmten Fällen.

Lopital ergreift Maßnahmen, um die Sicherheit und Vertraulichkeit von Daten bei der internationalen Übermittlung zu gewährleisten.

8. Sicherheitsmaßnahmen

Wir ergreifen angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten, darunter:

- Sichere Speicherung und Verschlüsselung von Daten;

- Zugriffskontrolle und Autorisierungsmanagement;
- Regelmäßige Audits und Updates;
- Richtlinien für das Vorfalldmanagement und Datenlecks;
- Multi-Faktor-Authentifizierung für kritische Konten oder Systeme;
- Regelmäßige Backups;
- Rollenbasierter Zugriff;
- SSL-Sicherheit;
- Passwortschutz und -richtlinien;
- Firewall;
- Protokollierung;
- Netzwerksegmentierung;
- Erkennung von Viren, Malware und Phishing;
- Automatische Updates und Patches;
- Erforderliche organisatorische Dokumentation;
- Protokoll und Register für Datenlecks;
- Cybersicherheits-Risikobewertung.

9. Rechte der betroffenen Personen

Betroffene Personen haben folgende Rechte:

1. Recht auf Auskunft – Artikel 15 DSGVO

Betroffene Personen haben das Recht zu erfahren, welche personenbezogenen Daten über sie verarbeitet werden und zu welchen Zwecken.

2. Recht auf Vergessenwerden (Recht auf Löschung) – Artikel 17 DSGVO

Betroffene können die Löschung ihrer personenbezogenen Daten verlangen, sofern keine gesetzliche Verpflichtung zur Aufbewahrung besteht.

3. Recht auf Berichtigung oder Ergänzung – Artikel 16 DSGVO

Betroffene können unrichtige oder unvollständige Daten berichtigen oder ergänzen lassen.

4. Recht auf Datenübertragbarkeit – Artikel 20 DSGVO

Betroffene Personen haben das Recht, ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und an eine andere Organisation weiterzugeben.

5. Recht auf Widerruf der Einwilligung – Artikel 7 Absatz 3 DSGVO

Wenn die Verarbeitung auf einer Einwilligung beruht, hat die betroffene Person das Recht, diese Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der Verarbeitung aufgrund der Einwilligung vor deren Widerruf berührt wird.

6. Recht auf Einschränkung der Verarbeitung – Artikel 18 DSGVO

Betroffene können unter bestimmten Umständen die vorübergehende Einschränkung der Verarbeitung ihrer personenbezogenen Daten verlangen, beispielsweise wenn die Richtigkeit der Daten bestritten wird.

7. Recht auf Widerspruch – Artikel 21 DSGVO

Betroffene können der Verarbeitung ihrer personenbezogenen Daten aufgrund berechtigter Interessen oder zu Direktmarketingzwecken widersprechen.

9.1 Regeln für Mitarbeiter

Die Regeln für Mitarbeiter sind in der Cyberhygiene-Richtlinie beschrieben.

10. Interne Verfahren bei Lopital

Bei Lopital gibt es unter anderem die folgenden internen Verfahren zur Gewährleistung der Cybersicherheit und Informationssicherheit:

- **Datenschutz-Audit:** AMVM Advies führt ein internes Datenschutz-Audit durch.
- **Verfahren bei Datenlecks:** Datenlecks werden gemäß Artikel 33 DSGVO innerhalb von 72 Stunden an die Datenschutzbehörde gemeldet.
- **Datenschutz durch Technik und durch Datenschutz in der Grundeinstellung:** Alle Systeme und Prozesse sind so konzipiert, dass der Datenschutz gewährleistet ist (Artikel 25 DSGVO).
- **Zwischenfallmanagement:** Ein Protokoll zur Identifizierung und Behebung von Sicherheitsvorfällen steht allen Mitarbeitern zur Verfügung.
- **Verarbeitungsregister:** Lopital führt ein Verzeichnis aller Datenverarbeitungsaktivitäten (Artikel 30 DSGVO).
- **Risikoanalyse und -management:** Lopital verfügt über eine Risikoanalyse, die sich auf interne Prozesse, Systeme, Daten und andere IT- und OT-Ressourcen konzentriert. Auf der Grundlage dieser Risikoanalyse werden Kontrollmaßnahmen getroffen, um die Risiken zu priorisieren und zu mindern.

11. Rollen und Verantwortlichkeiten

Innerhalb von Lopital gibt es Rollen und Verantwortlichkeiten in Bezug auf die DSGVO und die allgemeine Cybersicherheit. Nachstehend finden Sie eine Übersicht.

- **Geschäftsführer:** Endverantwortlich für die Einhaltung der DSGVO.
- **Finanzmanager:** Verantwortlich für die interne Kommunikation, die Einhaltung von Richtlinien und Verfahren.
- **AMVM-Beratung:** Verantwortlich für die Beratung und Unterstützung in Bezug auf Datenschutz und Cybersicherheit, wo erforderlich.
- **Allgemeiner Mitarbeiter:** Verantwortlich für den angemessenen Umgang mit personenbezogenen Daten und die Einhaltung von Richtlinien.

12. Änderungen dieser Richtlinie

Diese Datenschutzrichtlinie kann geändert werden. Die aktuellste Version ist stets verfügbar. Wichtige Änderungen werden vom Finanzmanager aktiv kommuniziert.