

# VERTROUWELIJKHEIDSBELEID MEDEWERKERS TAILORMATE

Dit is het “Vertrouwelijkheidsbeleid voor Medewerkers” van Tailormate BVBA (hierna “Tailormate”), een vennootschap naar Belgisch recht, met maatschappelijke zetel te Steenhoevestraat 8, 2800 Mechelen, met ondernemingsnummer 0875.797.459.

Deze Policy heeft betrekking op alle medewerkers, inclusief werknemers, freelancers, leden van het bestuur, het management, vrijwilligers, stagiairs, ... (hierna: “Medewerker”) en zodus iedereen die op de een of andere manier met vertrouwelijke informatie van Tailormate wordt geconfronteerd of met data die kunnen worden beschouwd als persoonsgegevens in de zin van Verordening 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (hierna “GDPR”).

Tijdens de uitoefening van hun respectieve functies bestaat de mogelijkheid dat Medewerkers worden geconfronteerd met vertrouwelijke informatie. Dit kan informatie zijn over Tailormate zelf, maar ook persoonsgegevens van leden, klanten, leveranciers en derden.

Dit vertrouwelijkheidsbeleid bevat de richtlijnen die alle Medewerkers in aanmerking dienen te nemen bij het uitoefenen van hun job.

## 1. WELKE INFORMATIE?

Als vertrouwelijke informatie in de zin van deze Privacy Policy wordt beschouwd:

- alle informatie van Tailormate die niet publiek is. Vertrouwelijke informatie die wederrechtelijk publiek werd gemaakt, dient eveneens beschouwd te worden als vertrouwelijke informatie. Zulke vertrouwelijke informatie omvat, maar is niet beperkt tot:
  - o alle tekeningen, formules, gedetailleerde beschrijvingen, boeken, software programma’s en hun broncode, handleidingen, dagrapporten, verslagen of notulen van vergaderingen, dagboeken en rekeningen, fabricatie- en handelsgeheimen, schriftelijke of mondelinge werkrichtlijnen, betreffende de activiteiten, methodes, processen, technieken of de uitrusting van Tailormate, haar moederverenootschap, dochterondernemingen of bijkantoren;
  - o alle informatie en documenten die door klanten ter beschikking wordt gesteld en alle hieruit voortvloeiende documenten, informatie, boekhouding, aangiften bij de overheid.
- alle persoonsgegevens zoals gedefinieerd door de Algemene Verordening Gegevensbescherming zijnde: *“alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon”*;

Hierna aangeduid als “Vertrouwelijke Informatie”.

## **2. TOEGANG TOT VERTROUWELIJKE INFORMATIE**

Tijdens de uitoefening van zijn job krijgt de Medewerker toegang tot Vertrouwelijke Informatie. De Medewerker is gehouden om deze Vertrouwelijke Informatie te allen tijde (zowel tijdens de (arbeids)overeenkomst als na de beëindiging van de (arbeids)overeenkomst) geheim te houden en enkel te delen met personen van wie werd geverifieerd of zij werden geautoriseerd om kennis te nemen van de Vertrouwelijke Informatie waarvan sprake. Alle Medewerkers zijn aldus voor al hun activiteiten in het kader van het kantoor gehouden tot de discretieplicht en de absolute naleving van het beroepsgeheim.

De Medewerker verbindt zich ertoe om geenszins Vertrouwelijke Informatie bewust of onbewust te delen met onbevoegde personen, inclusief derden.

In de praktijk moet elke Medewerker, bij twijfel over de naleving van het beroepsgeheim of van de discretieplicht, de persoon raadplegen die zijn werk superviseert en hem de situatie uiteenzetten waarmee hij wordt geconfronteerd. Indien nodig kunnen de verantwoordelijke en de Medewerker zich wenden tot Ignace Degens om hun verplichtingen in het betreffend geval te verduidelijken.

De Medewerker verbindt zich bovendien ertoe om deze Vertrouwelijke Informatie nooit te gebruiken in het nadeel van Tailormate of voor een ander doel dan dat van zijn opdracht.

## **3. BEHEER VAN VERTROUWELIJKE INFORMATIE**

- a. De Medewerker is zelf verantwoordelijk voor de juiste opslag van zijn bestanden en voor zijn eigen wachtwoord.

Dit impliceert dat de Medewerker:

- alle werk gerelateerde bestanden uitsluitend opslaat op de servers en zodus geenszins op de harde schijf van zijn lokale computer. Het systeem van Tailormate wordt immers regelmatig geüpdatet teneinde beveiligingsrisico's te ondervangen. Bovendien is er op deze manier ook geen verlies van data mogelijk aangezien er regelmatig een back-up wordt gemaakt van deze documenten.
- zijn computer vergrendelt met een sterk wachtwoord als hij zijn computer alleen laat (Ctrl - alt - delete: deze computer vergrendelen/lock computer). Een sterk wachtwoord is een wachtwoord van minstens 8 tekens, bestaat uit zowel kleine letters als minstens 1 hoofdletter, en ook minstens 1 cijfer.
- zijn mobiele toestellen (smartphone, tablet) beveiligt met een sterke toegangscode, voor zover dit toestel toegang heeft tot Vertrouwelijke Informatie.
- ieder beveiligingsprobleem waarvan hij/zij zich bewust wordt onmiddellijk dient te melden aan Ignace Degens.

- b. De Medewerker is ervoor verantwoordelijk om geen Vertrouwelijke Informatie te delen met onbevoegde personen.

Vooraleer de Medewerker Vertrouwelijke Informatie zou delen met andere Medewerkers of personen die anderszins tewerkgesteld zijn of een taak uitoefenen voor Tailormate dient de Medewerker er zich steeds van te vergewissen dat de persoon met wie hij deze Vertrouwelijke Informatie deelt, ook geautoriseerd is om toegang te krijgen tot deze informatie.

- c. De Medewerker verbindt zich ertoe zich geen toegang te verschaffen tot informatie waarvan hij redelijkerwijze behoort te weten dat hij geen recht heeft op toegang tot deze informatie.
- d. De Medewerker dient printopdrachten die Vertrouwelijke Informatie bevatten na het printen onmiddellijk van de printer te halen.
- e. De Medewerker verbindt zich ertoe om elke vorm van datalek of enige andere inbreuk op de GDPR, hoe gering ook, onmiddellijk aan de daartoe bevoegde persoon (m.n. Ignace Degens) te melden binnen Tailormate.

#### **4. TRANSPORT VAN VERTROUWELIJKE INFORMATIE**

Bij transport van Vertrouwelijke Informatie, bv. het meenemen van een USB-stick of laptop buiten de gebouwen van Tailormate, houdt de Medewerker rekening met de volgende richtlijnen:

- de Medewerker beperkt het transport van Vertrouwelijke Informatie tot een absoluut minimum en uitsluitend tot hetgeen strikt noodzakelijk is voor de uitvoering van zijn werk;
- de Medewerker dient zich te allen tijd bewust te zijn van het risico op verlies van data in een dergelijke situatie;
- de Medewerker dient al het mogelijke te doen om te voorkomen dat gegevens worden gestolen of verloren raken (bv. door het vergeten van laptop/smartphone op de trein, door diefstal van de laptop die in de wagen wordt achtergelaten,...);
- de Medewerker mag zijn computer nooit ergens onbeheerd achterlaten buiten de werkvloer;
- indien de Medewerker het slachtoffer wordt van diefstal van zijn laptop, smartphone of tablet, dient hij zijn leidinggevende onverwijld en uiterlijk 6 uur na het ontdekken ervan te verwittigen. Indien de Medewerker vaststelt dat zijn computer, tablet of smartphone werd gehackt, dient hij zijn leidinggevende onverwijld en uiterlijk binnen 6 uur na het ontdekken te verwittigen.
- indien de Medewerker gebruikt maakt van een ander draadloos netwerk dan het netwerk van Tailormate, dient hij te verifiëren of het een veilig netwerk betreft. De Medewerker zal bovendien in geen enkel geval gebruikmaken van een open en onbeveiligd wifinetwerk.

#### **5. CLEAN DESK POLICY**

Zodra een bureau of werkplek onbemand is voor een langere periode (d.i. vanaf een halve dag), dient de Medewerker rekening te houden met de volgende richtlijnen:

- alle Vertrouwelijke Informatie dient verwijderd te worden van het bureau of de werkplek en dient opgeslagen of gearchiveerd te worden in een afgesloten kast of locker. Dit geldt eveneens voor Vertrouwelijke Informatie die op een USB-stick, cd of dvd wordt bewaard.
- alle documenten die Vertrouwelijke Informatie bevatten en die voor de vuilnisbak bestemd zijn, dienen in de speciaal voorziene vuilnisbakken te worden gegooid OF dienen door de

papierversnipperaars te worden gehaald.

- computers dienen vergrendeld te worden wanneer het bureau of de werkplek niet bezet is en dienen volledig afgesloten te worden aan het einde van de werkdag.
- laptops, tablets en andere losse hardware devices moeten aan het einde van de werkdag in een locker of afgesloten kast worden opgeborgen.
- de sleutels van lockers en kasten mogen in geen geval onbewaakt achterblijven.

## **6. INZAGE IN COMPUTER/LAPTOP**

Het is verboden voor Medewerkers om de computer/laptop die door Tailormate ter beschikking wordt gesteld te gebruiken voor persoonlijke doeleinden. Meer bepaald is het verboden om documenten of gegevens te bewaren op de door Tailormate ter beschikking gestelde computer/laptop of om privé-e-mails te verzenden met het door Tailormate ter beschikking gestelde e-mailadres.