Informatiebeveiligingsbeleid AndMore Direct BV

Artikel 1 - Inleiding

1. AndMore Direct BV zet zich in voor de hoogste normen van informatiebeveiliging in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG).
2. Dit informatiebeveiligingsbeleid (hierna: het beleid) is uitsluitend bedoeld voor intern gebruik en referentie. Het is geen openbaar document en mag niet worden bekendgemaakt aan iemand buiten AndMore Direct BV. Het niet naleven van de AVG brengt AndMore Direct BV en zijn klanten in gevaar, en daarom neemt AndMore Direct BV de naleving van de AVG en dit beleid uiterst serieus.
3. De Privacy Officer (PO) is verantwoordelijk voor het toezicht op en de uitvoering van dit beleid. Als een medewerker vragen of opmerkingen heeft over de inhoud van dit beleid, kan hij contact opnemen met de PO via norbert@andmore.direct.
4. Dit doel van dit beleid is om:
5. AndMore Direct BV te beschermen tegen mogelijke inbreuken op de vertrouwelijkheid van interne gegevens
6. ervoor te zorgen dat alle informatiemiddelen en IT-faciliteiten van AndMore Direct BV worden beschermd tegen schade, verlies of misbruik
7. ervoor te zorgen dat al het personeel op de hoogte is van en voldoet aan de Nederlandse privacywetgeving (inclusief maar niet beperkt tot de AVG)
8. de procedures die van toepassing zijn op de verwerking van gegevens te ondersteunen
9. het bewustzijn en begrip bij het personeel van AndMore Direct BV te vergroten van de vereisten van informatiebeveiliging
10. de verantwoordelijkheid van het personeel van AndMore Direct BV te vergroten om de vertrouwelijkheid te waarborgen van de informatie die zij zelf verwerken

Artikel 2 - Toepassingsgebied

- De bedrijfsinformatie die onder dit beleid valt, omvat alle schriftelijke, gesproken en elektronische bedrijfsinformatie die wordt bewaard, gebruikt of verzonden door of namens het bedrijf, in welke media dan ook. Dit omvat bedrijfsinformatie op computersystemen, draagbare apparaten, telefoons, papieren dossiers en mondeling overgedragen informatie.
- Dit beleid is van toepassing op al het personeel, waaronder begrepen werknemers, uitzendkrachten, andere contractanten, stagiaires en vrijwilligers.
- Alle medewerkers moeten bekend zijn met dit beleid en zich houden aan de richtlijnen ervan.
- Dit beleid vormt een aanvulling op andere protocollen van AndMore Direct BV met betrekking tot gegevensbescherming en -beveiliging.
- Dit beleid maakt geen deel uit van de arbeidsovereenkomst van een werknemer en AndMore Direct BV kan dit beleid van tijd tot tijd aanvullen of wijzigen met aanvullende richtlijnen. Elk nieuw of gewijzigd beleid zal aan het personeel worden doorgegeven voordat het wordt geïmplementeerd.

Artikel 3 - Algemene principes

1. Alle bedrijfsinformatie moet worden behandeld als commercieel waardevol en worden beschermd tegen verlies, diefstal, misbruik of ongepaste toegang of openbaarmaking.
2. Het personeel moet met de managers de passende beveiligingsmaatregelen bespreken die geschikt en van kracht zijn voor het soort informatie waartoe zij toegang hebben tijdens de uitvoering van hun werkzaamheden.
3. Medewerkers moeten ervoor zorgen dat ze alle trainingen over informatiebeveiliging bijwonen waarvoor ze worden uitgenodigd, tenzij anders overeengekomen met hun manager.
4. Informatie is eigendom van AndMore Direct BV en niet van een medewerker of team.
5. Bedrijfsinformatie mag alleen worden gebruikt in verband met werk dat voor AndMore Direct BV wordt uitgevoerd en niet voor andere commerciële of persoonlijke doeleinden.

Artikel 4 - Informatiebeheer

1. De verzamelde informatie mag niet buitensporig zijn en moet adequaat, relevant, nauwkeurig en actueel zijn voor de doeleinden waarvoor het door AndMore Direct BV wordt gebruikt.
2. Informatie wordt niet langer bewaard dan nodig is in overeenstemming met de richtlijnen voor het bewaren van gegevens van AndMore Direct BV. Al het vertrouwelijke materiaal dat

moet worden verwijderd, moet worden versnipperd of, in het geval van elektronisch materiaal, op veilige wijze worden vernietigd, zodra de noodzaak voor bewaring is verstreken.

Artikel 5 - Personeelsinformatie

1. Gezien de interne vertrouwelijkheid van personeelsdossiers, is de toegang tot dergelijke informatie beperkt tot de afdeling Personeelszaken. Behalve zoals voorzien in individuele rollen, hebben andere medewerkers geen toegang tot die informatie.
2. Elk personeelslid in een management- of toezichthoudende rol moet personeelsinformatie vertrouwelijk behandelen.
3. Medewerkers kunnen vragen om inzage in hun personeelsdossiers in overeenstemming met de relevante bepalingen van de AVG.

Artikel 6 - Toegang tot kantoren en informatie

1. Kantoordeuren moeten te allen tijde beveiligd zijn en bezoekers mogen geen sleutels of toegangscodes krijgen.
2. Documenten die vertrouwelijke informatie bevatten en apparatuur die vertrouwelijke informatie weergeeft, moeten zo worden geplaatst dat ze niet kunnen worden bekeken door voorbijgangers, bijvoorbeeld door kantoorramen.
3. Bezoekers moeten worden verplicht zich aan te melden bij de receptie, te allen tijde vergezeld te worden en nooit alleen worden gelaten in ruimtes waar ze toegang kunnen hebben tot vertrouwelijke informatie.
4. Waar mogelijk vinden ontmoetingen met bezoekers plaats in vergaderruimten. Als het voor een personeelslid nodig is om bezoekers te ontmoeten in een kantoor of andere ruimte die bedrijfsinformatie bevat, moeten maatregelen worden genomen om ervoor te zorgen dat er geen vertrouwelijke informatie zichtbaar is.
5. Aan het einde van elke dag, of wanneer bureaus leeg zijn, moeten alle papieren documenten, back-upsystemen en apparaten die vertrouwelijke informatie bevatten, veilig worden opgeborgen.

Artikel 7 - Computers en IT

1. Werknemers gebruiken wachtwoordbeveiliging en encryptie waar beschikbaar op bedrijfssystemen om de vertrouwelijkheid te waarborgen.
2. Computers en andere elektronische apparaten moeten met een wachtwoord worden beveiligd en die wachtwoorden moeten regelmatig worden gewijzigd. Wachtwoorden mogen niet worden opgeschreven of aan anderen worden gegeven.
3. Computers en andere elektronische apparaten moeten worden vergrendeld wanneer ze niet worden gebruikt om het risico van onopzettelijk verlies of openbaarmaking te minimaliseren.
4. Vertrouwelijke informatie mag niet worden gekopieerd naar diskette, verwisselbare harde schijf, cd of dvd of geheugenstick zonder de uitdrukkelijke toestemming van de manager en zelfs dan moet deze worden versleuteld. Gegevens die naar een van deze apparaten zijn gekopieerd, moeten zo snel mogelijk worden verwijderd en worden opgeslagen op het computernetwerk van AndMore Direct BV zodat er een back-up van kan worden gemaakt.
5. Van alle elektronische gegevens moet aan het einde van elke werkdag een veilige back-up worden gemaakt.
6. Medewerkers moeten ervoor zorgen dat ze geen virussen of kwaadaardige code op bedrijfssystemen introduceren. Software mag niet van internet worden geïnstalleerd of gedownload zonder dat deze eerst op virussen is gecontroleerd. Medewerkers moeten contact opnemen met de IT-afdeling voor advies over de juiste stappen die moeten worden genomen om naleving te waarborgen.

Artikel 8 - Communicatie en overdracht

1. Elke medewerker moet voorzichtig zijn met het waarborgen van vertrouwelijkheid van bedrijfsinformatie wanneer ze in openbare ruimtes praten.
2. Vertrouwelijke informatie moet worden gemarkeerd als 'vertrouwelijk' en mag alleen worden verspreid onder degenen die de informatie nodig hebben in het kader van hun werk voor AndMore Direct BV.
3. Post-, fax- en e-mailadressen moeten worden gecontroleerd en geverifieerd voordat informatie wordt verzonden. Bijzondere aandacht moet worden besteed aan het invoeren van

e-mailadressen bij mailprogramma's waar de functies voor automatisch aanvullen mogelijk onjuiste adressen oplevert.
4. Alle gevoelige of vertrouwelijke informatie moet worden gecodeerd voordat deze per e-mail wordt verzonden, of worden verzonden per tracked DX of aangetekende verzending.
5. Gevoelige of vertrouwelijke informatie mag niet per fax worden verzonden, tenzij de werknemer er zeker van is dat deze niet op ongepaste wijze wordt onderschept op het faxapparaat van de ontvanger.
6. Vertrouwelijke informatie mag niet uit het kantoor van AndMore Direct BV worden meegenomen zonder toestemming van de relevante manager, behalve wanneer het meenemen tijdelijk en noodzakelijk is.
7. In de beperkte omstandigheden waarin het een werknemer is toegestaan om vertrouwelijke informatie uit het kantoor mee te nemen, moet hij alle redelijke maatregelen nemen om ervoor te zorgen dat de integriteit van de informatie en de vertrouwelijkheid worden gewaarborgd.
8. De werknemer moet in de situatie beschreven in het vorige lid ervoor zorgen dat vertrouwelijke informatie:
   a. niet wordt vervoerd in doorzichtige of andere onbeveiligde tassen of koffers
   b. niet gelezen worden op openbare plaatsen, zoals wachtkamer, café of trein
   c. niet onbeheerd wordt achtergelaten

Artikel 9 - Thuiswerken

1. De medewerker mag geen vertrouwelijke of andere bedrijfsinformatie mee naar huis nemen zonder de toestemming van de relevante manager en mag dit na deze toestemming alleen doen als er naar tevredenheid passende technische en praktische maatregelen zijn getroffen in het huis om de voortdurende veiligheid en vertrouwelijkheid van die informatie te waarborgen.
2. Een medewerker mag geen geen vertrouwelijke bedrijfsinformatie opslaan op thuiscomputers (pc's, laptops of tablets).
3. In de beperkte omstandigheden waarin het de werknemer is toegestaan bedrijfsinformatie mee naar huis te nemen, moet hij ervoor zorgen dat:
4. vertrouwelijke informatie wordt bewaard in een veilige en afgesloten omgeving waar deze niet toegankelijk is voor familieleden of bezoekers
5. al het vertrouwelijke materiaal dat moet worden verwijderd, moet worden versnipperd of, in het geval van elektronisch materiaal, veilig worden vernietigd zodra de noodzaak voor bewaring is verstreken

Artikel 10 - Doorgifte aan derden

1. Derde partijen mogen alleen worden gebruikt om bedrijfsinformatie te verwerken in omstandigheden waarin schriftelijke overeenkomsten zijn gesloten om ervoor te zorgen dat deze dienstverleners passende maatregelen voor informatiebeveiliging gegevensbescherming hebben getroffen.
2. Medewerkers die betrokken zijn bij het opzetten van nieuwe regelingen met derden of het wijzigen van bestaande regelingen dienen de PO te raadplegen voor meer informatie.

Artikel 11 - Overzeese doorgifte

- Er zijn beperkingen aan de internationale doorgifte van persoonsgegevens. Medewerkers mogen geen persoonlijke gegevens overdragen buiten de EER (EU, IJsland, Liechtenstein en Noorwegen) zonder eerst de juridische afdeling en de PO te raadplegen.

Artikel 12 - Inbreuken melden

Iedere medewerker is verplicht om feitelijke of potentiële tekortkomingen in de naleving van de gegevensbescherming aan de PO te melden. Dit stelt AndMore Direct BV in staat om:

- de tekortkoming te onderzoeken en indien nodig passende maatregelen te nemen
- eventuele relevante meldingen te maken

Artikel 13 - Gevolgen van niet-naleving

1. AndMore Direct BV neemt de naleving van dit beleid zeer serieus. Het niet naleven brengt ernstige risico's met zich mee voor zowel het personeel als AndMore Direct BV. Het belang

van dit beleid betekent dat het niet naleven van een van de regels ervan kan leiden tot disciplinaire maatregelen, waaronder ontslag.
2. Medewerkers met vragen of opmerkingen over iets in dit beleid kunnen contact opnemen met de PO via norbert@andmore.direct.

Artikel 14 - Ingang beleid
Dit informatiebeveiligingsbeleid gaat in op 26 maart 2023.