PRIVACY POLICY

1. DOEL VAN DE POLICY

FrontForce NV waardeert het recht op privacy en is gecommitteerd om te garanderen dat het verwerven, verwerken en gebruiken van alle Persoonlijke data zal gebeuren op een veilige, ethische en transparante manier die in overeenstemming is met de toepasselijke wetgeving.

Deze Policy is de basis voor alle privacy van persoonlijke data en zet de data beveiliging van FrontForce NV inzake bestuur en principes uiteen inzake het volgende

i. Verwerken en behandelen van persoonlijke data van huidige, vroegere en toekomstige werknemers, klanten, leveranciers, of andere derde partijen

ii. Bewaren van persoonlijke data op fysieke bestanden (bv papier) of in een elektronische vorm (e-mail of documenten gecreëerd met software applicaties)

Deze policy is van toepassing samen met andere policies en procedures.

2. DEFINITIES/AFKORTINGEN

Toepasselijke wetgeving	De verordening 2016/679 van het Europees Parlement en de Raad 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 en tot intrekking van Richtlijn 95/46/EC;
Verwerkings-verantwoordelijke	De natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan dat, alleen of met anderen, de doelen en middelen tot verwerking van persoonlijke data bepaalt.
Verwerker	Een natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt
Betrokkene	Geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegevens betrekking hebben;

Persoonsgegevens	Alle gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene(n)”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met

	name aan de hand van en 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;
Verwerking	een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens
Ontvanger	Een natuurlijke of rechtspersoon, overheidsinstantie, een dienst of ander orgaan, aan wie de persoonlijke data geopenbaard worden
Gevoelige persoonsgegevens	Persoonsgegevens bestaande uit informatie over zijn/haar etnische oorsprong, politieke en filosofische overtuigingen, religieuze overtuigingen, lidmaatschap van vakbond en posities in vakbonden, fysieke of mentale gezondheid, seksuele voorkeur, administratieve of criminele veroordelingen, sociale zekerheid documenten, rijksregisternummer, bankrekeningnummer die identiteitsdiefstal kunnen vergemakkelijken.

3. SAMENVATTING VAN VERANTWOORDELIJKHEDEN

HR of de DPO zullen de algemene toepassing van deze policy overzien, met name;

- Aanbevelingen tot aanpassing van deze policy wanneer wetgeving of context verandert
- Samenwerken met de juridische dienst, IT, HR en andere functies in het kader van data privacy;
- Ontwikkelen en voorzien in communicatie en training
- Advies verlenen aan management inzake data privacy;
- Escaleren naar management bij significante compliance problemen en mitigatieplannen, alsook de implicaties van privacy wetgeving

4. BESCHRIJVING VAN DE POLICY

a. Verwerking van persoonsgegevens

FrontForce NV neemt de volgende passende stappen om de veiligheid van privacy te garanderen:

i. Alle persoonlijke date wordt verwerkt in overeenstemming met de toepasselijke lokale wetgeving, professionele standaarden en alle toepasselijke lokale polices, met in acht name van de wettelijke rechten van de relevante persoon

ii. Waar noodzakelijk door de Toepasselijke Wetgeving, zullen de relevante personen informatie ontvangen over de doeleinden van de verwerking, de identiteit van de verwerkingsverantwoordelijke, de ontvangers of categorieën van ontvangers van de persoonsgegevens en andere informatie die noodzakelijk is zodat de verwerking van persoonsgegevens in lijn is met de standaarden zoals uiteen gezet in deze policy.

iii. Waar gevraagd door de Toepasselijke Wetgeving, zal instemming gevraagd worden indien dit noodzakelijk is voor het verwerking van persoonsgegevens van de relevante betrokkenen.

iv. Inzake gevoelige persoonsgegevens zullen additionele maatregelen toegepast worden. Specifiek:

- Gevoelige persoonsgegevens zouden niet verzameld moeten worden indien dit niet noodzakelijk is voor de doeleinden waarvoor de data is verzameld of verwerkt,
- Toegang moet beperkt worden tot de noodzakelijke personen,
- Vragen van expliciete toestemming waar noodzakelijk

b. Verwerkingsprincipes

FrontForce NV verwerkt persoonsgegevens in lijn met de Toepasselijke Wetgeving en in overeenstemming met de volgende data beschermingsprincipes

i. **Rechtmatigheid, eerlijkheid en transparantie**: Verwerken van persoonlijke data in een rechtmatige, eerlijke en transparantie manier.

ii. **Doelbeperking**: Persoonsgegevens worden enkel verwerkt voor het doeleinde gespecifieerd op het tijdstip van collectie. Wijzigingen in het doeleinde zijn enkel in beperkte mate mogelijk en zullen, over het algemeen, toestemming vereisen.

iii. **Data minimalisatie:** Verwerking van persoonsgegevens die adequaat en relevant zijn voor de doeleinden waarvoor we de data verwerken. Iedere verwerking van persoonsgegevens zal gelimiteerd worden tot datgene wat noodzakelijk is om de doeleinden te verwezenlijken. Waar het doeleinde het toelaat en waar uitgaven in verhouding zijn met het te bereiken doen, zal geanonimiseerde of gepseudonimiseerde data gebruikt worden. Persoonsgegevens zullen niet pro-actief verzameld worden en zullen niet bewaard worden voor toekomstige doeleinden, tenzij dit noodzakelijk is of toegalaten wordt door de Toepasselijke Wetgeving.

iv. **Accuraatheid:** Onjuiste of onvolledige data zal vernietigd, aangepast of vervolledigd worden.

v. **Opslag beperking:** Persoonsgegevens zullen niet langer dan noodzakelijk voor de doeleinden van verwerking, bijgehouden worden. Data die niet langer nodig is na de vervaldatum van wettelijke of ondernemingsprocessen, zal verwijderd worden. Personal data will not be kept longer than is necessary for the purposes for which personal data is processed. Data that is no longer needed after the expiration of legal or business process related periods will be deleted. Er kan een indicatie zijn dat informatie dient beschermd te worden in bepaalde gevallen. Indien dit het geval is, zullen we dat data bijhouden tot het geschil wettelijk is uitgeklaard.

vi. **Integriteit en confidentialiteit:** Persoonsgegevens zullen op zo een manier verwerkt worden die garant staat voor de noodzakelijke veiligheid van data, inclusief bescherming tegen ongeautoriseerde of onwettelijke verwerking en tegen het onopzettelijk verlies, vernietiging of schade, gebruik makend van de noodzakelijke technische en organisatorische maatregelen.

c. Rechtsgronden

De Toepasselijke Wetgeving eist van FrontForce NV dat zij transparant is over de rechtsgronden of de rechtvaardiging voor het verwerken van persoonsgegevens. Hieronder geven wij de belangrijkste wettelijke rechtvaardigingen die van toepassing zijn op onze verwerking van persoonsgegevens:

i. Noodzakelijk voor de uitvoering van een contract

ii. Wettelijke verplichting die FrontForce NV moet nakomen

iii. Rechtvaardig belang

iv. Instemming

d. Delen van data

Persoonsgegevens moeten mogelijks geopenbaard worden aan andere noodzakelijke personen (zo genoemde “derde partijen ontvangers”).

FrontForce NV moet de persoonsgegevens aan derde partijen ontvangers openbaren, enkel als zij zeker is van een adequaat niveau van gegevensbescherming. In alle gevallen, moet de toegang en de transfer van persoonsgegevens beperkt worden naar individuen die dit moeten weten. Derde partijen ontvangers acteren onder een bindende verplichting data enkel te verwerken voor de afgesproken doeleinden en om de persoonsgegevens te beschermen door het toepassen van maatregelen gelijkaardig aan de maatregelen vermeld in deze policy.

e. Grensoverschrijdende overdracht van persoonsgegevens

Persoonsgegevens kunnen mogelijks moeten overgebracht worden naar landen buiten de Europese Economisch Unie die niet de noodzakelijke bescherming van persoonsgegevens bieden.

Indien persoonsgegevens van de Europese Economische Unie naar een land buiten de Unie, dat niet de noodzakelijke bescherming van persoonsgegevens biedt, moeten overgebracht worden, dienen passende waarborgen geïmplementeerd te worden gelijkaardig aan de standaarden van deze privacy policy. <Naam bedrijf> zal verantwoordelijk blijven voor het verwerken van persoonsgegevens en zal de noodzakelijke maatregelen nemen om de verwerking hiervan te beschermen (door bv. Standard contract clausules).

f. Data retentie

Persoonsgegevens mogen niet langer dan noodzakelijk voor de doeleinden waarvoor de data werd verzameld bijgehouden worden. De exacte periode zal afhangen van het doel waarvoor we de data bijhouden. Bijkomend, zijn er wetten en voorschriften die van toepassing zijn en welke een minimum retentie periode van persoonsgegevens vaststellen.

g. Rechten van de betrokkene

Betrokkenen hebben het recht om:

i. Informatie te verkrijgen over het al dan niet verwerken van persoonsgegevens, en indien er sprake is van verwerking, toegang te verkrijgen tot hun persoonsgegevens en informatie met betrekking tot de verwerking;

ii. Incorrecte persoonsgegevens te corrigeren, te vervolledigen en het recht om de ontvangers van de persoonsgegevens op de hoogte te brengen van de rechtzetting;

iii. Bezwaar aan te tekenen tegen de verwerking van persoonsgegevens gebaseerd op welbepaalde gronden en het recht om ten alle tijde bezwaar te maken tegen het gebruik van persoonsgegevens voor direct marketing doeleinden;

iv. In het geval van geautomatiseerde beslissing name, een menselijke interventie te bekomen, een mening te geven, uitleg te verkrijgen inzake de geautomatiseerde beslissing en de beslissing te betwisten; en

v. In het geval van het verlenen van toestemming voor de verwerking van persoonsgegevens, het recht om de toestemming ten alle tijd in te trekken, zonder dat het intrekken hiervan impact heeft op de rechtmatige verwerking gebaseerd op toestemming voor de intrekking.

Onder bepaalde omstandigheden, hebben betrokkenen ook het recht om

i. Persoonsgegevens te laten verwijderen;

ii. Het verwerken van persoonsgegevens te beperken, en in het geval van beperking, de verwerking de limiteren tot louter opslag;

iii. Persoonsgegevens te verstrekken.

h. Confidentialiteit

Persoonsgegevens zullen verwerkt worden op een strikte “moet weten basis”, dit betekent dat persoonsgegevens enkel verwerkt zullen worden en medewerkers enkel toegang zullen hebben tot persoonsgegevens wanneer dit passend en noodzakelijk is voor het type en de scope van de taak in kwestie. Het is verboden voor medewerkers om persoonsgegevens te gebruiken voor eigen persoonlijk of commercieel doel, om persoonsgegevens vrij te geven aan ongeautoriseerde personen, of om ze beschikbaar te maken in iedere andere vorm.

i. Veiligheid

Geschikte technische, fysieke en organisatorische maatregelen die redelijk zijn ontworpen om persoonsgegevens te beschermen tegen onvrijwillige of onrechtmatige vernietiging, verlies, wijziging, ongeautoriseerde toegang, en tegen andere onrechtmatige vormen van verwerking, moeten toegepast worden. Toegang tot persoonsgegevens is beperkt tot geautoriseerde ontvangers op een “moet weten basis”. Bijkomend, het onderhoud van een informatiebeveiligingsbeleid in verhouding tot de vastgestelde risico’s gelinkt tot verwerking, zou in plaats moeten zijn. Veiligheidsprogramma’s moeten constant aangepast worden om operationele risico’s te mitigeren en persoonsgegevens te beschermen, rekening houdend met industry accepted practices.

j. Communicatie, awareness, training

Wij zullen redelijke en geschikte stappen ondernemen om de vereisten van deze privacy policy te communiceren en training te voorzien.

5. ESCALATIES

Het niet volgen van deze Privacy Policy kan significante veiligheidsrisico’s inzake confidentialiteit, integriteit en beschikbaarheid van (gevoelige) informatie introduceren en kan tijdelijk of permanent schade toebrengen aan de reputatie van FrontForce NV.

Het niet volgen van deze Privacy Policy en de geassocieerde procedures kan mogelijks leiden tot disciplinaire acties zoals uiteen gezet in het arbeidsreglement.

Iedere medewerker die gevraagd wordt een taak uit te voeren die in strijd is met deze Privacy Policy moet, zo snel als mogelijk, contact opnemen met zijn direct leidinggevende of de DPO.

Afwijkingen of uitzondering op deze Privacy Policy zijn enkel toegestaan na een formeel risico assessment dat de impact van de afwijking of uitzondering heeft vastgesteld, waarbij het risico formeel is geaccepteerd door de informatie eigenaar en wanneer formele goedkeuring is verkregen.