Privacybeleid

Aanduiding
In dit document duiden wij onszelf aan met “ons”, “wij”, “we” of “onze”.

Website
Als wij het hebben over de website dan wordt daarmee bedoeld: www.stichtingbethlehem.nl

Rechtmatigheid en doelen van de verwerking
a. Wij verwerken persoonsgegevens omdat en voor zover dat noodzakelijk is:
- voor de verwerking van donaties,
- voor de communicatie met donateurs die daar prijs op stellen,
- voor de uitvoering van de overeenkomsten met onze werknemers, veldwerkers, zendingswerkers en vrijwilligers.
- Voor de uitvoering van (overige) overeenkomsten.

b. We verwerken niet meer persoonsgegevens dan nodig is.
c. Ontvangers van onze nieuwsbrieven hebben de mogelijkheid zich hiervoor af te melden.
d. We verstrekken geen persoonsgegevens aan derden, tenzij dat noodzakelijk is.

Bijzondere persoonsgegevens
Wij verwerken bijzondere persoonsgegevens, namelijk ID-bewijzen. We realiseren ons dat het hier gaat om bijzondere persoonsgegevens. Alle gegevens moeten we met de grootste zorg behandelen, maar deze helemaal.

Ons eigen personeel, veldwerkers, zendingswerkers en vrijwilligers
Van ons eigen personeel (waaronder ook veldwerkers, zendingswerkers en vrijwilligers die vergoeding van ons ontvangen) verwerken we persoonsgegevens ter uitvoering van de (arbeids)overeenkomsten en om te voldoen aan de wettelijke plichten. Denk hierbij aan zaken als het uitbetalen van salaris, het doorgeven van informatie aan de belastingdienst en het doen van afdrachten. We verstrekken zo nodig ook persoonsgegevens aan de arbodienst c.q. bedrijfsarts. Als we méér gegevens verwerken, maken we dat kenbaar inclusief de reden ervan. We verwerken ook persoonsgegevens als we beoordelingsgespreksverslagen en andere documenten/berichten over het functioneren van het personeel maken en in het personeelsdossier voegen. We doen dat dan om het functioneren vast te leggen en zo nodig te verbeteren. Ook hebben we (voor zover relevant) verzuimdossiers. We verwerken alleen die persoonsgegevens die wettelijk gezien nodig zijn om te verwerken of als het nodig is om de verplichtingen uit de (arbeids)overeenkomsten na te komen.

Doorgifte
Indien wij persoonsgegevens doorgeven aan een entiteit in een land buiten de Europese Unie, gaan we na of de betreffende entiteit aldaar een passend beschermingsniveau waarborgt.

Functionaris gegevensbescherming
Wij hebben geen functionaris gegevensbescherming in de zin van de AVG.

PARAAF _____

PRIVACYBELEID STICHTING BETHLEHEM

Privacyverklaring
Jegens derden geldt onze privacyverklaring, waarvan de (laatste versie) op onze website staat.

Bewaartermijnen
De door ons gehanteerde bewaartermijnen staan vermeld in de privacyverklaring.

Technische en organisatorische beveiligingsmaatregelen
Wij hebben onder andere de volgende technische en organisatorische maatregelen ter bescherming van de persoonsgegevens tegen verlies of onrechtmatige verwerking:

Technische maatregelen:

1. Computers en laptops zijn voorzien van wachtwoorden. Voor inloggen in de systemen is een ander wachtwoord nodig. We werken met tweefactorauthenticatie.
2. Wachtwoorden worden periodiek veranderd en dienen complex te zijn.
3. Er is sprake van een goede virusscanner en firewall.

Organisatorische maatregelen:

1. Medewerkers worden gestimuleerd om niet onnodig veel data te verzamelen.
2. Het is werknemers verboden om persoons- en klantgegevens buiten de normale systemen op hun eigen laptop, computer, telefoon, usb-stick of anderszins op te slaan.
3. Toegang van ex-medewerker tot systemen wordt beëindigd.
4. We werken met verschillende rechtengroepen. Wie ergens geen belang bij heeft, krijgt er ook geen toegang toe.

Geheimhouding en instructie personeel
Persoonsgegevens mogen alleen worden verwerkt in opdracht van ons.

Onze opdracht is om bij het verwerken van persoonsgegevens de regels uit dit privacy beleid (dit document) en de privacyverklaring (zie nogmaals de website) na te leven.

Het is elke van onze werknemers (daarom) verboden, zowel gedurende het dienstverband als na afloop daarvan, op enigerlei wijze, direct of indirect, persoonsgegevens van (één van) onze werknemers, veldwerkers, zendingswerkers, vrijwilligers, bestuursleden en/of donateurs of andere relaties te verwerken, anders dan in opdracht van ons. Onze regels moeten worden nageleefd.

Onder ‘verwerken’ wordt alles verstaan wat mogelijk is, zoals opslaan, opvragen, wissen, doorsturen, inzien, bewerken, ordenen.

PARAAF _____

PRIVACYBELEID STICHTING BETHLEHEM

Datalekken
Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden melden we dat binnen 72 uur na het ontdekken aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoud voor de rechten en vrijheden van natuurlijke personen delen wij de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee. Als **bijlage 1** is ons Protocol datalekken toegevoegd.

Versie van dit document
Wij zijn gerechtigd dit document in de loop van de tijd zo nodig aan te passen. Telkens is de laatste versie van toepassing.

Ondertekening
Iedere werknemer en bestuurslid dient kennis te nemen van de inhoud van dit document en van de genoemde bijlagen en naar de inhoud hiervan te handelen. Daarom zal dit document door iedere werknemer en bestuurslid worden ondertekend en iedere pagina worden geparafeerd.

Bijlage:
1: Protocol datalekken

Ondertekend door: **op:**

HANDTEKENING _____

BIJLAGE 1

Protocol datalekken

1. Regelgeving
De meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken in voorkomende gevallen datalekken moeten melden aan de Autoriteit Persoonsgegevens (AP) en in bepaalde gevallen ook aan de betrokkene.

2. Wat is een datalek?
Een datalek is het gevolg van een beveiligingsincident maar niet ieder beveiligingsincident is een datalek. Als alleen sprake is van een zwakke plek in de beveiliging spreken we van een beveiligingslek en niet van een datalek.

Een datalek wordt in de AVG omschreven als een 'inbreuk in verband met persoonsgegevens'. De definitie hiervan is: **„inbreuk in verband met persoonsgegevens"**: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

Een paar voorbeelden van een datalek:
- Een kwijtgeraakte USB-stick waarop persoonsgegevens staan;
- een kwijtgeraakt papieren dossier met donateursgegevens of bankgegevens
- een gestolen laptop;
- een inbraak door een hacker;
- een malware-besmetting;
- een calamiteit zoals een brand bij een datacenter.
- Een e-mail met persoonsgegevens die naar een verkeerde ontvanger is verzonden en door die ontvanger is ingezien.

3. Interne procedure melding datalek
De meldplicht datalekken regelt dat een datalek uiterlijk binnen 72 uur na het ontdekken van het lek gemeld moet worden aan de AP. Deze melding behoeft niet te worden gedaan als het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Het is voor ons als organisatie en voor jou als medewerker dan ook van belang dat je een (vermoedelijk) datalek direct meldt bij I. Jonkers of bij P. Hoogendijk.

Wanneer een melding achterwege blijft terwijl dit wel had gemoeten, mag de Autoriteit Persoonsgegevens hoge boetes opleggen: Deze bestuurlijke boete bedraagt maximaal 4% van de jaaromzet. Twijfel je over de ernst van het datalek? Neem dan te allen tijde contact op met één van de zojuist genoemde personen.

PARAAF _____

BIJLAGE 1: PROTOCOL DATALEKKEN

Bij een melding van het datalek benoem je (voor zover bekend) de navolgende punten:
1. het moment van het (vermoedelijke) datalek;
2. de feiten en gegevens omtrent de (beveiligings)inbreuk;
3. de aard en de omvang van de gegevens die het betreft.

Wanneer er sprake blijkt te zijn van een datalek, worden er maatregelen getroffen om dit in de toekomst te voorkomen en wordt het datalek eventueel door ons gemeld bij de AP.

4. Verdere maatregelen die van belang zijn
Om de persoonsgegevens waarover wij beschikken te beschermen, gelden onder andere de volgende maatregelen:
- Iedere 6 maanden dienen wachtwoorden en andere inloggegevens van de computer, te worden gewijzigd;
- Het is niet toegestaan zakelijke apparatuur voor privé doeleinden te gebruiken.
- Vanuit kantoor worden geen (financiële) gegevens verzonden via andere kanalen dat wat gebruikelijk is.

5. Documentatie
Iedere datalek moet door ons worden gedocumenteerd. Dit zal gebeuren door I. Jonkers.

6. Melding aan betrokkene
Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet de inbreuk onverwijld aan de betrokkene te worden meegedeeld. Dit behoeft niet wanneer één van de volgende voorwaarden is vervuld (artikel 34 lid 3 AVG):

a. de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

b. de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

c. de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

PARAAF _____