Raad voor maatschappelijk welzijn
Zitting van 22 oktober 2024
Notule

Aanwezig: Steven De Maesschalck: voorzitter;
Kurt Windels: burgemeester;
Martine Verhamme, Trui Lambrecht, Jan Rosseel: leden van het vast bureau;
Nadine Verheye: schepen;
Katrien Vandecasteele: lid van het vast bureau (voorzitter BCSD);
Jan Defreyne, Sabine Lampaert, Filip Blanckaert, Enigo Vandendriessche, Carine Geldhof, Bart Buyse, Lucas Staes, Ann Vandevelde, Diederik Vanderheeren, Kurt Soenens, Evy Becquart, Liesbeth Holvoet, Koen Depreiter, Rudi Debruyne: raadsleden;
Dominik Ronse: algemeen directeur

De zitting vangt aan om 20.30 uur.

De heer Steven De Maesschalck, voorzitter, deelt mee dat, in uitvoering van artikel 32 van het Decreet over het Lokaal bestuur van elke raadszitting een zittingsverslag dient te worden gemaakt. Dit zal gebeuren aan de hand van een audio-opname van de zitting. Deze zitting zal samen met de notulen gepubliceerd worden overeenkomstig 286 van het Decreet over het Lokaal bestuur.

Openbare zitting

1. Goedkeuren van de notulen van de vorige zitting

De RAAD VOOR MAATSCHAPPELIJK WELZIJN,

Gelet op het Decreet over het Lokaal bestuur, meer bepaald artikel 74;

Gelet op het Decreet over het Lokaal bestuur, meer bepaald de artikels 277 en 278;

Gelet op de ontwerpnotulen van de vorige zitting, opgesteld door de algemeen directeur;

Op voorstel van de voorzitter van de raad voor maatschappelijk welzijn;

BESLUIT:

eenparig

Artikel 1 – De notulen van de vorige zitting worden goedgekeurd.

Artikel 2 – Aan de algemeen directeur wordt de opdracht gegeven deze notulen op te nemen in het register van beraadslagingen van de raad voor maatschappelijk welzijn.

Beslissingen

ALGEMEEN BESTUUR

2. Goedkeuren van het informatieveiligheidsplan

De RAAD VOOR MAATSCHAPPELIJK WELZIJN,

Gelet op het Decreet over het Lokaal bestuur;

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Privacywet);

Gelet op het decreet van 8 juni 2018 houdende de aanpassing van de decreten aan de verordening (EU) 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/EG (algemene verordening gegevensbescherming);

Gelet op de beslissing van de raad voor maatschappelijk welzijn van 21 september 2021 houdende goedkeuren van het informatieveiligheidsplan;

Overwegende dat het tweede informatieveiligheidsplan, na verlopen van de termijn, vervangen moet worden door een nieuw plan;

Gelet op de verwezenlijkingen van het eerste en tweede informatieveiligheidsplan waarmee gemeente en OCMW zich konden conformeren aan de verplichtingen inzake informatieveiligheid;

Overwegende dat de gemeente en het OCMW een gezamenlijk traject hebben doorlopen voor het opstellen van het derde informatieveiligheidsplan op basis van de aangepaste regelgeving en de resterende knelpunten;

Overwegende dat het informatieveiligheidsplan een actieplan is dat op basis van een organisatiebrede risico-analyse de nodige te nemen maatregelen beschrijft met de daaraan gekoppelde timing;

Gelet op het ontwerp van informatieveiligheidsplan opgesteld door de functionaris voor gegevensbescherming en na unaniem advies van de informatieveiligheidscel;

Op voorstel van de voorzitter van het vast bureau;

BESLUIT:

eenparig

Artikel 1 – Het informatieveiligheidsplan wordt goedgekeurd en als bijlage bij deze beslissing gevoegd.

Informatieveiligheidsplan 2024-2027

Gemeente en OCMW Ingelmunster

DPO	C-smart
Versie	2024.2
Datum	10/09/2024
IV Scan door	Lowie Van Hooreweder

Inhoud

1. Inleiding

In het digitale tijdperk is een robuust informatieveiligheidsbeleid essentieel voor lokale besturen. De toenemende afhankelijkheid van technologie en digitalisering biedt aanzienlijke voordelen, maar vergroot ook de kwetsbaarheid voor cyberaanvallen, datalekken en andere beveiligingsrisico's. Deze risico's kunnen leiden tot ernstige financiële, reputatie- en operationele schade.

Informatieveiligheid betreft de bescherming van informatie en informatiesystemen tegen ongeautoriseerde toegang, gebruik of bekendmaking, accidentele wijziging, vernietiging en verlies door noodsituaties. Dit omvat het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en het voorkomen van vervalsing en verlies van legitieme informatie. Een informatieveiligheidsbeleid biedt een overzicht van de geïdentificeerde risico’s en de manieren waarop deze worden afgedekt. Het implementeren van een dergelijk beleid versterkt het vertrouwen van burgers en partners in de diensten van lokale besturen, onderstreept hun toewijding aan informatieveiligheid en draagt bij aan een veiligere digitale omgeving voor iedereen.

Een effectief informatieveiligheidsbeleid beschermt niet alleen gevoelige informatie tegen ongeautoriseerde toegang en misbruik, maar zorgt ook voor naleving van wettelijke en regelgevende vereisten op het gebied van privacy en gegevensbescherming. Lokale besturen moeten voldoen aan de geldende privacywetgeving, waaronder de Algemene Verordening Gegevensbescherming (GDPR). Europese, federale en Vlaamse overheden stellen strenge normen voor het gebruik en de bescherming van persoonsgegevens. De Gegevensbeschermingsautoriteit (GBA) geeft voortdurend nieuwe adviezen uit. Voor de OCMW ‘s gelden ook de strikte voorwaarden van de Minimale Normen KSZ. Net als bij het vereiste veiligheidsplan voor welzijn op het werk en ongevallenpreventie, is een openbaar bestuur wettelijk verplicht een functionaris voor gegevensbescherming aan te stellen en een meerjarenplan voor informatieveiligheid op te stellen. Dit plan moet jaarlijks worden geactualiseerd. Zowel de federale als de Vlaamse overheid kunnen deze veiligheidsplannen specifiek opvragen en inspecteren.

Begin 2024 heeft het lokaal bestuur de procedure gestart voor het opstellen van een nieuw informatieveiligheidsplan 2024-2027. Voor de opmaak van dit plan heeft de DPO een risicoanalyse uitgevoerd, gebaseerd op de richtsnoeren van de Autoriteit Gegevensbescherming, die voortbouwen op de ISO 27000-norm. Deze risicoanalyse omvatte een documentenanalyse, een focusgesprek met verschillende medewerkers en een interview met de ICT-dienst. Hieruit volgden aanbevelingen om de informatieveiligheid van het lokaal bestuur te verbeteren.

Het informatieveiligheidsplan 2024-2027 begint met onze visie op informatieveiligheid, gevolgd door een uiteenzetting over het beheer hiervan, inclusief de rol van de informatieveiligheidscel en de functionaris voor gegevensbescherming. Vervolgens worden de geplande acties verduidelijkt.

2. Beleidsverklaring gegevensbescherming

Het lokaal bestuur is een informatieverwerkende organisatie. Burgers, medewerkers, bedrijven en verenigingen geven hun ('gevoelige') informatie aan het bestuur en het bestuur heeft betrouwbare informatie nodig om haar taken te kunnen uitvoeren. Daarom moet de beschikbare informatie op een veilige en alerte manier verwerkt worden.

Informatieveiligheid beschermt deze informatie tegen een brede waaier van bedreigingen. Zo verzekert ze de continuïteit van de organisatie, beperkt ze mogelijke schade en draagt ze maximaal bij tot de realisatie van de bestuurlijke doelstellingen. Informatieveiligheid is essentieel om het vertrouwen van de burgers in het bestuur te versterken.

Gegevensbescherming is meer dan het implementeren van technische en organisatorische oplossingen. Een belangrijke pijler is het bewust maken van alle personeelsleden binnen het bestuur, zodat zij dit beleid begrijpen en toepassen. Dit geldt ook voor mandatarissen, externen (leveranciers, onderaannemers, consultants…), stagiairs, jobstudenten en vrijwilligers. Informatiebeveiliging is een kernopdracht voor alle betrokken partijen binnen het bestuur. Het is een taak van iedereen.

In die zin streeft het bestuur naar een geïntegreerde systeemaanpak, met als resultaat dat de risico's voor de confidentialiteit[1], integriteit[2], beschikbaarheid[3], proportionaliteit[4], finaliteit[5], legaliteit[6] en auditeerbaarheid[7] van de informatiebronnen en –systemen tot een minimum beperkt blijven.

Het bestuur ontwikkelt het gegevensbeschermingsbeleid in overeenstemming met de geldende privacywetgeving, zijnde de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en de Europese Verordening 2016/679 van 27 april 2016 betreffende de bescherming van de natuurlijke personen met betrekking tot het verwerken van persoonlijke gegevens en het vrije verkeer van deze gegevens.

Het gegevensbeschermingsbeleid is terug te vinden in de privacyverklaring van het bestuur. Voor de uitvoering van dit beleid verwijzen we naar dit informatieveiligheidsplan. Dit plan wordt opgevolgd door de informatieveiligheidscel en gecoördineerd door de functionaris gegevensbescherming.

[1] Waarborgen dat de informatie alleen toegankelijk is voor wie daartoe bevoegd is.
[2] Het beveiligen van de nauwkeurigheid en volledigheid van informatie en verwerkingsmethoden.
[3] Waarborgen dat bevoegde gebruikers wanneer dat nodig is toegang hebben tot informatie.
[4] De persoonsgegevens moeten toereikend, ter zake dienend en niet overmatig zijn, uitgaand van de doeleinden waarvoor ze verkregen/verwerkt worden. Ze mogen niet langer worden bewaard dan noodzakelijk.
[5] De persoonsgegevens moeten voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen en mogen niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden.
[6] De verwerking van persoonsgegevens mag uitsluitend op een eerlijke en rechtmatige wijze gebeuren.
[7] Het gebruik en het raadplegen van gegevens moet sporen achterlaten, controleerbaar zijn.

3. Het informatieveiligheidsbeheer

Lokale besturen zijn wettelijk verplicht om onder andere te beschikken over een functionaris voor gegevensbescherming (DPO), een informatieveiligheidsplan (IVP) en een informatieveiligheidsbeheersysteem.

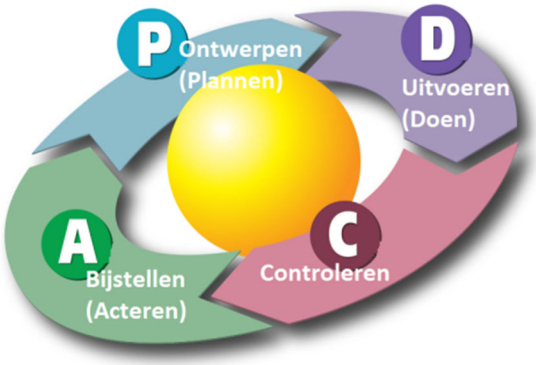
Het lokaal bestuur van Ingelmunster stelde C-smart aan als functionaris voor gegevensbescherming. De opdracht wordt uitgevoerd door Lieselot Hemeryck. Qua budget kan het bestuur rekenen op een jaarlijkse begeleiding van 10 dagen beleidsondersteuning vanuit C-smart.

Het informatieveiligheidsbeheer is in handen van de informatieveiligheidscel die minstens viermaal per jaar vergadert. Het informatieveiligheidsteam is samengeteld uit volgende personen:

- Functionaris voor gegevensbescherming: C-smart
- Algemeen directeur: Dominik Ronse
- Coördinator organisatiebeheer: Christophe Pareit
- Deskundige burgerzaken: Marieke Maertens
- Coördinator zorg en welzijn: Christine Vandevoorde
- Beleidsondersteuner gemeentescholen: Tine Maes
- Coördinator technische dienst - preventieadviseur: Wim Decoopman
- Dienst IT: Wouter Verhelst
- Systeembeheerder: Rik Vansteenkiste
- Deskundige personeel: Charlotte Demarez
- Schepen IT: Jan Rosseel
- Burgemeester: Kurt Windels

De veiligheidscel heeft een adviserende, stimulerende, documenterende en controlerende opdracht. Dat wil zeggen:

- Plan: de veiligheidscel maakt het veiligheidsplan.
- Do: de veiligheidscel coördineert de uitvoering (wie doet welke acties tegen wanneer).
- Check: de veiligheidscel volgt na elk kwartaal de voortgang op.
- Act: de veiligheidscel stuurt de planning bij waar nodig.



De veiligheidscel borgt de afgeronde acties die een meerwaarde zijn voor het bestuur door ze structureel in te passen in de werking. Naast de coördinatie van het veiligheidsplan, bespreekt de veiligheidscel eventuele informatieveiligheidsincidenten die zich hebben voorgedaan en de afhandeling daarvan en stelt beveiligingsmaatregelen voor.

Jaarlijks stelt de functionaris voor gegevensbescherming een verslag op bestaande uit:

- Een algemeen overzicht van de veiligheidstoestand, de ontwikkeling in het afgelopen jaar en de nog te realiseren doelstellingen;
- Een samenvatting van de adviezen die aan de verantwoordelijke van het dagelijks bestuur werden bezorgd en het gevolg dat eraan werd gegeven;
- Een overzicht van de werkzaamheden, verricht door de functionaris;
- Een overzicht van de resultaten van de controles, uitgevoerd door de functionaris;
- Een overzicht van de gevoerde campagnes ter bevordering van de veiligheid;
- Een overzicht van alle gevolgde en geplande opleidingen.

In het kader van haar controlerende taak zal de informatieveiligheidscel volgend auditplan toepassen met betrekking tot haar informatieveiligheidsbeleid:

- Jaarlijkse logcontrole RR en KSZ;
- Jaarlijkse zelfevaluatie via de vragenlijst van de KSZ;
- Driejaarlijks conformiteitsaudit informatieveiligheid waarbij de volgende audit uitgevoerd zal worden in Q2 2027.

4. Informatieveiligheidsplan

In het informatieveiligheidsplan zijn de acties voor de periode 2024-2027 opgenomen. We onderscheiden (1) acties die permanente of jaarlijkse aandacht vragen, (2) acties voor 2024, (3) acties voor 2025, (4) acties voor 2026 en (5) acties voor 2027.

4.1 Acties die permanente of jaarlijkse aandacht vragen

Actie	Wie	Timing
Het bestuur houdt de adviezen, instructies en eisen vanuit de toezichthoudende autoriteit in het oog inzake Informatieveiligheid en de uitvoering van de GDPR.	IVC	Permanent
Het bestuur dient permanent aandacht te hebben voor de rechten en vrijheden van de burgers wiens gegevens zij verwerken. Bij een hoog risico op hun rechten dient er een gegevensbeschermingseffectbeoordeling uitgevoerd te worden.	IVC	Permanent
Het bestuur meet en monitort haar incidenten om beveiligingsrisico's te reduceren. Het bestuurt informeert alle medewerkers en mandatarissen actief over de incidentenprocedure.	IVC	Permanent
De Informatieveiligheidscel komt actief om de drie maanden bijeen om het veiligheidsplan op te volgen.	IVC	Permanent
Bij alle nieuwe samenwerkingsverbanden (leverancier, intergemeentelijke samenwerkingsverband,..) formaliseert het bestuur de verwerking van persoonsgegevens via de daarvoor meest passende document (verwerkingsovereenkomst, protocol, regeling gezamenlijke verwerkingsactiviteit, gebruikersovereenkomst of vertrouwelijkheidsovereenkomst).	IVC	Permanent
Dienst ICT zal gestructureerd overleggen met de DPO zodoende Informatieveiligheid meegenomen wordt in verbeterprojecten, nieuwe verwerkingen en aankoop nieuwe hard- en software. Waar nodig zal de DPO een gegevensbeschermingseffectbeoordeling uitvoeren.	ICT/DPO	Permanent
Informatieveiligheid zal als een vast agendapunt opgenomen worden in het MT.	IVC	Permanent
De IVC volgt de actuele onderwerpen op die invloed hebben op de informatieveiligheid. De onderwerpen kunnen als extra acties worden toegevoegd aan het informatieveiligheidsplan.	IVC	Permanent
De DPO maakt het jaarverslag op van het voorafgaand jaar.	DPO	Jaarlijks
Het lokaal bestuur voert jaarlijks een logcontrole uit van de raadpleging van de authentieke bronnen.	IVC/DPO	Jaarlijks
Voer regelmatige bewustwordingscampagnes uit over cyber hygiëne, inclusief het vermijden van verdachte links en het updaten van software. Moedig consistent goede beveiligingspraktijken aan bij alle medewerkers.	IVC	Permanent
Het lokaal bestuur zal jaarlijks haar UPS'en testen.	IVC	Jaarlijks

4.2 Acties voor 2024

Actie	Wie	Timing
Voer een gedetailleerd onderzoek uit naar de voordelen van het implementeren van een wachtwoordkluis. Focus op hoe deze kan helpen bij het genereren en beheren van sterke wachtwoorden en het veilig delen van inloggegevens binnen het team.	ICT	Q3
Organiseer bewustwordingscampagnes om medewerkers te leren hoe ze sterke wachtwoordzinnen kunnen maken. Benadruk het gebruik van langere, gemakkelijk te onthouden zinnen in plaats van korte en complexe wachtwoorden.	IVC	Q3
Plan regelmatig trainingen over het gebruik van belangrijke platformen zoals Teams, SharePoint en gedeelde schijven. Richt je op het juiste gebruik voor verschillende taken en hoe medewerkers deze optimaal kunnen benutten.	ICT	Q3
Bevorder het gebruik van Teams/sharepoint-links voor het delen van bestanden om beveiligingsrisico's en e-mailbijlageproblemen te verminderen. Verspreid richtlijnen en voordelen van deze methode onder medewerkers.	ICT/IVC	Q4
Ontwikkel en communiceer een duidelijk beleid voor het versnipperen van gevoelige documenten. Dit moet richtlijnen omvatten over wanneer en hoe fysieke documenten veilig vernietigd moeten worden. Sensibiliseer rond het versnipperen. Zorg hierbij dat dit wordt uitgebreid voor elektronische dragers.	DPO, Archief en ICT	Q4
Betrek raadsleden actief bij bewustwordingscampagnes over informatieveiligheid. Zorg ervoor dat ze goed geïnformeerd zijn over hun rol en verantwoordelijkheden in het beveiligen van informatie.	IVC	Q4

4.3 Acties voor 2025

Actie	Wie	Timing
Voer BitLocker-encryptie uit op alle nieuwe apparaten om gevoelige gegevens te beschermen.	ICT	Q1
Onderzoek en implementeer privacyfolie op ramen op het gelijkvloers om inkijk van buitenaf te voorkomen. Dit helpt bij het beschermen van vertrouwelijke informatie die binnenkant zichtbaar zou kunnen zijn. Dit zou voornamelijk een probleem zijn op donkere winterdagen.	DPO	Q1
Plan en voer regelmatige technische audits uit om de effectiviteit van beveiligingsmaatregelen te evalueren. Identificeer en adresseer eventuele kwetsbaarheden of verbeterpunten.	DPO	Q1
Stel een gedetailleerd overzicht op van wie welke rechten heeft binnen elke toepassing en wie de beheerder is. Gebruik bestaande tools zoals Topdesk voor een efficiënte inventarisatie en beheer.	DPO	Q2
Schrijf duidelijke richtlijnen uit voor het gebruik van foto’s. Dit voor zowel het vragen van de toestemming op verschillende evenementen, als het gebruik op de site en andere publicaties.	DPO	Q2
Implementeer een honeypot om als lokmiddel te dienen voor kwaadwillenden, waardoor je netwerkbeveiliging wordt versterkt en verdachte activiteiten vroegtijdig worden gedetecteerd.	ICT	Q3
Evalueer en herstructureer het huidige sleutelbeheerplan om te verzekeren dat alleen geautoriseerde personen toegang hebben tot gevoelige gebieden. Dit omvat het bijwerken van wie sleutels bezit en waarvoor ze toegang hebben.	IVC	Q4
Stel een uitgebreid incident response plan op dat duidelijke stappen bevat voor het reageren op beveiligingsincidenten. Wijs rollen en verantwoordelijkheden toe en zorg voor regelmatige oefeningen om paraatheid te testen.	DPO/ICT	Q4

4.4 Acties voor 2026

Actie	Wie	Timing
Er wordt een backup- en recoveryplan opgesteld. Voer periodieke tests uit van back-up systemen om de integriteit en betrouwbaarheid van gegevensherstel te waarborgen. Documenteer de resultaten en verbeter processen indien nodig.	ICT	Q1
Organiseer regelmatig tabletop-oefeningen om incident response scenario's te simuleren. Deze oefeningen helpen teams om effectiever te reageren op echte beveiligingsincidenten door het verbeteren van hun coördinatie en reactiesnelheid.	IVC	Q1
Het lokaal bestuur overweegt de mogelijkheden van secure DNS.	IVC/ICT	Q2
Het bestuur zal toestellen met een antivirus met slechte status weren van het netwerk.	ICT	Q2
Er wordt een data classificatiesysteem opgezet. Prioriteer de middelen van de organisatie, zoals hardware, apparaten, data, tijd, personeel, informatie en software, op basis van hun classificatie, kriticiteit en bedrijfswaarde. Beoordeel de impact van openbaarmaking, beschadiging, verlies of verminderde integriteit van deze middelen en rangschik ze dienovereenkomstig.	ICT/IVC	Q3
Voer een externe pentest audit uit om de risico’s en gebreken in kaart te brengen.	ICT	Q3
Ontwikkel en onderhoud een uitgebreide strategie voor het beheren van informatie- en cybersecurityrisico's als onderdeel van het algehele risicobeheer van de organisatie. Documenteer en keur deze risico's formeel goed, en update ze bij veranderingen. Zorg voor de juiste toewijzing van middelen ter bescherming van bedrijfskritische activa en overweeg het gebruik van risicomanagementtools.	DPO	Q4

4.5 Acties voor 2027

Actie	Wie	Timing
Het dataregister wordt geüpdatet met de nieuwe verwerkingen, de aangepaste verwerkingen of verwerkingen die niet meer voorvallen worden er uit gehaald.	DPO	Q1
Er zal een uitgebreide analyse van het gebouw worden uitgevoerd. Deze analyse heeft tot doel om een grondig inzicht te verkrijgen in de verschillende aspecten van het gebouw, waaronder de architectuur, infrastructuur, beveiligingsmaatregelen en mogelijke risicofactoren. Door middel van deze gebouwenanalyse kunnen we de veiligheid en het welzijn van de aanwezigen verbeteren door passende maatregelen te implementeren op basis van de verkregen inzichten.	DPO	Q1
Het bestuur start met de opmaak van een nieuwe Informatieveiligheidsplan.	DPO	Q2

SOCIALE ZAKEN

3. Goedkeuren van een subsidiereglement houdende het voorzien van een toelage ter bevordering van de e-inclusie van kansengroepen

De RAAD VOOR MAATSCHAPPELIJK WELZIJN,

Gelet op het Decreet over het Lokaal bestuur van 22 december 2017;

Gelet op het besluit van de Vlaamse Regering van 15 juli 2022 waarbij een nieuwe subsidie werd goedgekeurd voor de (verdere) uitrol van het lokale e-inclusiebeleid door Vlaamse steden en gemeenten en de Vlaamse Gemeenschapscommissie;

Gelet op het feit dat de gemeente Ingelmunster in samenwerking met DVV Midwest een e-inclusieproject lopende heeft;

Gelet op het feit dat er voor Ingelmunster een bedrag van 7.599,90 euro voorzien is als trekkingsrecht om te besteden aan het bevorderen van de individuele toegang tot het internet voor kwetsbare burgers;

Overwegende dat er een reglement wordt voorgesteld om een toelage van 50 euro te voorzien voor de kwetsbare burgers die voldoen aan de gestelde voorwaarden voor de besteding van dit bedrag;

Op voorstel van de bevoegd lid van het vast bureau;

BESLUIT:

eenparig

Artikel 1 – Het reglement voor de toelage ter bevordering van de digitalisering wordt goedgekeurd en als bijlage toegevoegd bij deze beslissing.

SUBSIDIEREGLEMENT TER BEVORDERING VAN DE E-INCLUSIE VAN KANSENGROEPEN

Algemene bepalingen

Artikel 1

De gemeente Ingelmunster voorziet een toelage met als doel de digitalisering van de burgers met financiële nood te bevorderen.

Deze toelage kadert in het actieplan 'Iedereen Digitaal' van de Vlaamse regering, waarvoor de gemeente Ingelmunster in samenwerking met DVV Midwest ondersteund wordt.

Voorwaarden

Artikel 2

De begunstigde moet voldoen aan de volgende voorwaarden:

- Domicilie in Ingelmunster;
- Gebruik maken van de voedselbedeling
  of
  een duidelijk financiële nood hebben volgens het sociaal onderzoek uitgevoerd door de maatschappelijk werker van het OCMW;
- Een digiscan laten uitvoeren door DVV Midwest
  Een digiscan is een onderzoek, aan de hand van een huisbezoek, waarbij de medewerker in kaart brengt wat er zoal in de woning te vinden is van digitale aspecten, van apparatuur tot facturatie, specifiek voor internet, telefonie en televisie. Ook de digitale kennis van de bewoner(s) wordt in kaart gebracht.

Aanvraag van de toelage

Artikel 3

De toelage moet aangevraagd worden tijdens een bezoek in het sociaal huis via het hiervoor voorziene aanvraagformulier.

Dit formulier kan verkregen worden via de balie of via een maatschappelijk werker van het OCMW.
In de aanvraag verklaart de begunstigde zich akkoord met een financieel onderzoek en met het uitvoeren van een digiscan.

Procedure

Artikel 4

Het aanvraagformulier moet de facturen van internet, telefonie en televisie bevatten.

De maatschappelijk werker bevestigt de financiële nood van de begunstigde op het aanvraagformulier.

Het aanvraagformulier bevat het rapport van de uitgevoerde digiscan.

De beslissing tot toekenning gebeurt door het bijzonder comité voor de sociale dienst.

De toelage wordt, na goedkeuring door het bijzonder comité voor de sociale dienst, binnen de maand gestort op het rekeningnummer van de aanvrager vermeld op het aanvraagformulier.

Uiterste datum van aanvragen

Artikel 5

Alle aanvragen met de nodige bewijzen moeten ingediend worden voor 1 mei 2025.

Bedrag van de toelage

Artikel 6

De toelage bedraagt 50 euro per adres en is éénmalig.

De toelage wordt toegekend binnen de beperkingen gesteld door het budget.

Betwisting

Artikel 7

Bij betwisting kan de begunstigde een verzoek tot heroverweging indienen bij het vast bureau. Het vast bureau beslist over de betwisting binnen de maand na het indienen van het verzoek.

Budget

Artikel 8

De raad voor maatschappelijk welzijn voorziet het budget voor deze toelage in het meerjarenplan van het OCMW.
DVV Midwest zal deze kost co-financieren vanuit het e-inclusieproject 'Iedereen Digitaal' met het bedrag dat aan de gemeente Ingelmunster is toegewezen.

(Reglement aangenomen door de raad voor maatschappelijk welzijn op 22 oktober 2024)

De zitting werd afgerond om 20.35 uur.

Dominik Ronse
algemeen directeur

Steven De Maesschalck
voorzitter

Digitaal ondertekend door: Dominik Ronse
Tijdstip: 2024.11.25 13:25:32 +01:00

Digitaal ondertekend door: Steven De Maesschalck
Tijdstip: 2024.11.21 16:22:06 +01:00