BIJLAGE 8 – GEGEVENSBESCHERMING

AFDELING 1. PERSOONSGEGEVENS VAN WERKNEMERS

Artikel 1 – Wettelijk kader

In deze afdeling wordt de medewerker op de hoogte gebracht van de verwerkingsactiviteiten die het Lokaal Bestuur Bilzen-Hoeselt kan doorvoeren met diens persoonsgegevens.

Het Lokaal Bestuur Bilzen-Hoeselt gebruikt en verwerkt de persoonsgegevens van de medewerker in overeenstemming met de Algemene Verordening Gegevensbescherming (hierna: **AVG**), namelijk *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*.

Artikel 2 – Contactgegevens

De medewerker kan contact opnemen met Lokaal Bestuur Bilzen-Hoeselt:

- Per post, naar Deken Paquayplein 1, 3740 Bilzen-Hoeselt
- Via het contactformulier op onze website
- Per e-mail, op het mailadres info-veiligheid@bilzen.be

De contactgegevens van onze Functionaris Gegevensbescherming (DPO) zijn:

C-Smart
privacy@c-smart.be

Artikel 3 – Definities bij verwerking van persoonsgegevens

Persoonsgegevens worden in artikel 4 van de AVG gedefinieerd als:
“Alle informatie betreffende een identificeerbare persoon die direct of indirect kan worden geïdentificeerd”
In eenvoudigere bewoordingen betekent dat voor de medewerker, alle informatie over de medewerker die het mogelijk maakt de medewerker te identificeren.

De definitie van ‘verwerking’ van persoonsgegevens kan ook worden geconsulteerd in artikel 4 van de AVG. In vereenvoudigde termen is het elke bewerking of geheel van bewerkingen die het Lokaal Bestuur Bilzen-Hoeselt kan doorvoeren met betrekking tot de persoonsgegevens van de medewerker (bv. verzamelen, opslaan, wijzigen, raadplegen, gebruiken, verspreiden, wissen, enz…)

Artikel 4 – Categorieën van persoonsgegevens

De categorieën van persoonsgegevens die het Lokaal Bestuur Bilzen-Hoeselt verwerkt van de medewerkers zijn:

- **Persoonlijke identificatiegegevens**, nl. voornaam, familienaam, adres, titel/functie, rijksregisternummer/identificatienummer van de sociale zekerheid, geboortedatum en geboorteplaats
- **Communicatiegegevens**, nl. (persoonlijk) e-mailadres, telefoonnummer
- **Gegevens inzake loonverwerking en bezoldiging**

- **Gegevens met betrekking tot het personeelsdossier**, nl. CV, opleiding en vorming, beroep en betrekking, samenstelling van het gezin
- **Badge**
- **Camerabeelden**

Daarenboven kan het Lokaal Bestuur Bilzen-Hoeselt 'bijzondere categorieën van persoonsgegevens' van de medewerker verwerken, namelijk gezondheidsgegevens.

Artikel 5 – Bron van de persoonsgegevens

De meeste persoonsgegevens uit artikel 4 verzamelt het Lokaal Bestuur Bilzen-Hoeselt bij de medewerker zelf, dat betekent:

- Ofwel dat het Lokaal Bestuur Bilzen-Hoeselt de gegevens bij de betrokkene heeft verzameld via waarneming (bv camerabeelden via cameratoezicht)
- Ofwel dat de medewerker deze zelf bewust heeft verstrekt aan het Lokaal Bestuur Bilzen-Hoeselt (bv. Communicatiegegevens)

Sommige persoonsgegevens uit artikel 4 verzamelt het Lokaal Bestuur Bilzen-Hoeselt bij derden of openbare bronnen, zoals de Kruispuntbank.

Artikel 6 – Rechtsgronden met betrekking tot de verwerking van persoonsgegevens

De persoonsgegevens van de medewerker bedoeld in artikel 4 kunnen worden verwerkt op één of meerdere van volgende rechtsgronden:

- De uitvoering van een contract tussen het Lokaal Bestuur Bilzen-Hoeselt en de medewerker
- De gerechtsvaardigde belangen van het Lokaal Bestuur Bilzen-Hoeselt, nl.
    - Om te kunnen reageren op verzoeken, vragen of opmerkingen of om contact op te kunnen nemen met de medewerker voor vragen of mededelingen van welke aard ook (**communicatiegegevens**)
    - Om adviesbijstand te verkrijgen inzake de arbeidskosten van de organisatie
    - Om welzijn op het werk van de medewerkers te kunnen waarborgen
    - De bescherming en uitoefening van onze wettelijke rechten
    - Om de veiligheid en gezondheid van de medewerkers (arbeidsongevallen, agressie tegen medewerkers, enz.) en de bescherming van de goederen van het Lokaal Bestuur Bilzen-Hoeselt (beschadiging, inbraak of ongeoorloofde toegang, diefstal, enz.) te waarborgen (**camerabewaking op de werkvloer**)
- Noodzakelijk om te voldoen aan een wettelijke verplichting die op het Lokaal Bestuur Bilzen-Hoeselt rust. Het gaat daarbij om wettelijke verplichtingen die op een werkgever rusten, bepalingen van het personeelsstatuut van het Lokaal Bestuur Bilzen-Hoeselt, alsook verplichtingen uit fiscale wetgeving
- Noodzakelijk voor doeleinden inzake sociale zekerheid (**gezondheidsgegevens**)

Artikel 7 – Verwerkingsdoeleinden

De persoonsgegevens uit artikel 4 kunnen worden verwerkt voor één of meerdere van volgende verwerkingsdoeleinden:

- Ten behoeve van een goede loonadministratie
- Bestelling maaltijdcheques
- Om de DIMONA-aangifte te kunnen doen
- Vorming en coaching van de medewerker met het oog op een goede personeelsadministratie
- Tijdsregistratie, nl. met het oog op registratie van de werkuren en controle op de werkplaats

- Toepassing van de sociale zekerheid (werkloosheid, uitkeringen, loonadministratie, aanvraag zorgkrediet, aanvraag, Vlaamse ondersteuningspremies, aanvraag thematische verloven, aanvraag/beheer pensioenen)
- Beheren van het personeelsdossier met het oog op een goede personeelsadministratie
- Beheren mandatarissen met het oog op het onderhouden van een algemene administratie inzake presentiegelden, pensioenen, lonen, verzekering, enz.
- Waarborgen welzijn op het werk nl via medische onderzoeken van het personeel, het beheer van verzekeringen inzake arbeidsongevallen en hospitalisatie, aanvragen medische controles, RIZIV-berekeningen
- Om adviesbijstand te krijgen voor de organisatie omtrent arbeidskosten
- Het bijhouden van een personeelslijst om een overzicht te krijgen op het volledig personeelsbestand en met het oog op een risicobepaling van de werkposten
- Administratieve verwerking en opvolging opleidingen in het kader van preventie
- Analyseren en documenteren arbeidsongevallen
- Organiseren en onderhouden overleg tussen werkgever en vakbonden ter preventie in het kader van psychosociaal welzijn op de werkvloer
- Opmaken verslagen van seksueel ongewenst gedrag en pesterijen ter preventie van psychosociale risico's
- Bijhouden en opvolgen van agressieve uitingen van derden tegenover medewerkers

Artikel 8 – Verwerkers

Een verwerker is een natuurlijk persoon of rechtspersoon die persoonsgegevens verwerkt op vraag van of in naam van het Lokaal Bestuur Bilzen-Hoeselt. Lokaal Bestuur Bilzen-Hoeselt kan soms een contract afsluiten met deze partij om bepaalde producten en/of diensten te leveren. Met andere woorden: Lokaal Bestuur Bilzen-Hoeselt doet een beroep op verwerkers, omdat dit noodzakelijk is voor de dienstvoering. In dit geval zal Lokaal Bestuur Bilzen-Hoeselt met de verwerker een schriftelijke overeenkomst aangaan waarbij de veiligheid van uw persoonsgegevens wordt gewaarborgd door de verwerker. De verwerker handelt steeds volgens de instructies van Lokaal Bestuur Bilzen-Hoeselt

Artikel 9 – Doorgifte van persoonsgegevens aan derden

De verwerking van persoonsgegevens houdt ook in dat in een aantal gevallen deze gegevens worden doorgegeven aan derden. Deze derden zijn sociale zekerheidsinstellingen, het Rekenhof, consultancy-bedrijven en verzekeringsmaatschappijen.
Het Lokaal Bestuur Bilzen-Hoeselt zal enkel noodzakelijke gegevens doorgeven aan deze derden (met inbegrip van andere per wet geautoriseerde instanties). Die doorgifte kan plaatsvinden op grond van één of meerdere van de volgende rechtsgronden:

- Noodzakelijk voor het uitvoeren van een contract tussen de medewerker en het Lokaal Bestuur Bilzen-Hoeselt
- Om aan een wettelijke verplichting te kunnen voldoen die op het Lokaal Bestuur Bilzen-Hoeselt rust
- Het gerechtvaardigd belang van het Lokaal Bestuur Bilzen-Hoeselt om adviesbijstand te krijgen met betrekking tot haar organisatie (bv inzake arbeidskosten)

Artikel 10 – Internationale doorgifte (buiten EER) van de persoonsgegevens

Het Lokaal Bestuur Bilzen-Hoeselt zal de persoonsgegevens van de medewerker alleen opslaan of overdragen binnen de Europese Economische Ruimte (de "EER"). De EER bestaat uit alle EU-lidstaten

plus Noorwegen, IJsland en Liechtenstein. Dit betekent dat de persoonsgegevens volledig beschermd zullen zijn onder de AVG of volgens gelijkwaardige wettelijke normen.

Artikel 11 – Rechten van de medewerker

De medewerker heeft op grond van de AVG bepaalde rechten betreffende diens persoonsgegevens. Deze rechten zijn:

- Het recht op inzage
- Het recht om onjuiste persoonsgegevens te laten verbeteren of onvolledige persoonsgegevens te laten vervolledigen
- Het recht om persoonsgegevens te laten verwijderen
- Het recht om de verwerking te beperken
- Het recht om bezwaar te maken tegen de verwerking
- Het recht op gegevensportabiliteit

Deze rechten zijn niet absoluut, kunnen complex zijn en niet alle details zijn hier opgenomen. Voor een volledige uitlegging van deze rechten, leest de medewerker daarom best de relevante bepalingen en richtlijnen van toezichthoudende autoriteiten (Hoofdstuk III van de AVG en https://www.gegevensbeschermingsautoriteit.be/burger)

De medewerker kan de rechten uitoefenen door middel van een schriftelijke kennisgeving aan het Lokaal Bestuur Bilzen-Hoeselt via mail op het e-mailadres info-veiligheid@bilzen.be

Het Lokaal Bestuur Bilzen-Hoeselt dient op het verzoek van de medewerker te reageren binnen een maand na ontvangst van dat verzoek. Normaal gesproken streeft het Lokaal Bestuur Bilzen-Hoeselt ernaar om binnen die tijd een volledig antwoord te geven. In sommige gevallen, vooral als het verzoek complexer is, kan er echter meer tijd nodig zijn, tot een maximum van drie maanden vanaf de datum waarop het Lokaal Bestuur Bilzen-Hoeselt het verzoek ontvangt. De medewerker wordt volledig op de hoogte gehouden van de voortgang.

Als de medewerker van mening is dat de verwerking van diens persoonsgegevens door het Lokaal Bestuur Bilzen-Hoeselt in strijd is met de AVG, heeft deze het recht om een klacht in te dienen bij een toezichthoudende autoriteit die verantwoordelijk is voor de gegevensbescherming.
In België is de toezichthoudende autoriteit de Gegevensbeschermingsautoriteit (GBA).

Gegevenbeschermingsautoriteit (GBA)
Drukpersstraat 35
1000 BRUSSEL
+32 (0)2 274 48 00
Contact@apd-gba.be
https://www.gegevensbeschermingsautoriteit.be

Artikel 12 – Beveiligingsmaatregelen en bewaartermijnen

Het Lokaal Bestuur Bilzen-Hoeselt neemt de nodige beschermings- en beveiligingsmaatregelen zowel op organisatorisch als technisch vlak met het oog op de bescherming van de persoonsgegevens. Behalve de persoonsgegevens voor welke het Lokaal Bestuur Bilzen-Hoeselt onderworpen is aan wettelijke bewaartermijnen, bewaart het persoonsgegevens niet langer dan strikt nodig voor de doeleinden waarvoor ze zijn verzameld. Overige persoonsgegevens die niet aan wettelijke bewaartermijnen zijn gebonden, worden na 3 jaar verwijderd.

AFDELING 2. PERSOONSGEGEVENS VAN DERDEN

2.1 GEDRAGSCODE VOOR ALLE MEDEWERKERS

Artikel 13 – Algemeen

In het kader van de bescherming van persoonsgegevens, is de medewerker verantwoordelijk voor het veilig beheer van persoonsgebonden informatie. Hij leeft de dienstnota's aangaande informatieveiligheid na.

- De medewerker verwerkt enkel persoonsgegevens in functie van een rechtmatig doel dat kadert binnen een wettelijke opdracht, een taak van algemeen belang of waarvoor toestemming van betrokkenen verkregen is.
- De medewerker verwerkt enkel de persoonsgegevens die nodig zijn voor het uitvoeren van zijn opdracht en zorgt ervoor dat deze altijd correct en volledig zijn.
- De medewerker deelt geen persoonsgegevens met derde partijen zonder wettelijke basis of toestemming van betrokkenen.
- Medewerkers erkennen hun verantwoordelijkheid in het veilig omgaan met persoonsgegevens en stellen zich waakzaam op om te vermijden dat onbevoegden zich toegang verschaffen tot persoonsgegevens.
- Medewerkers verbinden zich ertoe om incidenten (een datalek) en inbreuken tegen het beleid voor de bescherming van persoonsgegevens te melden aan hun leidinggevenden.

Voor de uitoefening van zijn opdracht krijgt elke medewerker de nodige ICT-middelen toegewezen. Het gaat zowel over systemen (hardware en software) als toegang tot communicatienetwerken (internet, gsm abonnement,...). De medewerker verbindt er zich toe om de toegewezen middelen te gebruiken als een goede huisvader. Hij houdt daarbij rekening met de geldende wetgevingen inzake informatieveiligheid en privacy en met alle interne richtlijnen die door leidinggevenden zijn opgelegd.

Het bestuur kan de naleving van het correct gebruik van de ICT-middelen controleren met alle middelen die wettelijk toegelaten zijn. Misbruik kan gesanctioneerd worden volgens de regels opgenomen in het arbeidsreglement.

2.2 GEDRAGSCODE VOOR INFORMATIEBEHEERDERS

Artikel 14 – Algemeen

Deze gedragscode schetst een kader voor alle informatiebeheerders van het lokaal bestuur van Bilzen-Hoeselt.
Het bestuur kan ten alle tijde het naleven van deze gedragsregels controleren. Het niet naleven van deze gedragscodes kan leiden tot een disciplinair proces.

Een informatiebeheerder is iedere persoon die in het kader van verantwoordelijkheden met betrekking tot een ICT-systeem over toegangsrechten beschikt die ruimer zijn dan het louter dagelijks functioneel gebruik van de informatie of het programma. Het gaat onder meer om toegangsbeheerders, systeembeheerders, databank administrators, informatieveiligheidsconsulenten (CISO), functionarissen voor de gegevensbescherming (DPO), softwareontwikkelaars en –beheerders, netwerkbeheerders, consultants, externe IT dienstenleveranciers en onderaannemers.

Artikel 15 – De ethische integriteit van de informatiebeheerder

De informatiebeheerder stelt zich objectief en onpartijdig op tijdens de uitoefening van zijn/haar functie.
De informatiebeheerder streeft ernaar (de perceptie van) persoonlijke belangenconflicten te vermijden. Wanneer deze zich toch voordoen, zal hij zijn diensthoofd daarover onmiddellijk inlichten en hierover een formele beslissing vragen.
De informatiebeheerder stelt zijn vaardigheden op gepaste wijze ten dienste van de organisatie en van de medewerkers van de informatiesystemen.

De informatiebeheer streeft ernaar in de best mogelijke verstandhouding samen te werken met alle medewerkers van de organisatie.

De informatiebeheerder zal zijn technische vaardigheden eerlijk voorstellen en doet een beroep op bijkomende professionele (technische) bijstand indien nodig.

De informatiebeheerder krijgt de middelen en levert voldoende inspanningen om op de hoogte te blijven van de evoluties binnen zijn/haar domein.

De informatiebeheerder zal met de (toezichthoudende) autoriteiten samenwerken.

Artikel 16 – De integriteit en de beschikbaarheid van de informatie

De informatiebeheerder waakt over het behoorlijk functioneren van het systeem en stelt de handelingen die nodig zijn om de integriteit en de beschikbaarheid van het informatiesysteem te garanderen.
De informatiebeheerder waakt erover dat de genomen acties niet het verlies, de onbeschikbaarheid of de vernietiging van de gegevens of van de toepassingen tot gevolg hebben.

Aangezien bepaalde handelingen van medewerkers schade kunnen berokkenen aan de integriteit of de beschikbaarheid van het informaticasysteem, moet de informatiebeheerder toezien op de naleving van het beleid ter zake. Indien nodig verwittigt hij/zij het diensthoofd. Indien hij/zij vaststelt dat bepaalde van deze acties niet onder het toepassingsgebied van de bestaande minimale normen vallen, brengt hij/zij de functionaris voor gegevensbescherming hiervan op de hoogte. Deze zal dan de nodige maatregelen treffen in het belang van de organisatie.

De informatiebeheerder zorgt ervoor dat de toegang tot het systeem gegarandeerd wordt aan de personen die dergelijke toegang nodig hebben in het kader van hun functie en dat de toegang tot die personen beperkt blijft.

Artikel 17 – Informatiebescherming

De informatiebeheerder is zich bewust van het feit dat hij/zij toegang heeft tot grote hoeveelheden persoonsgegevens en gevoelige gegevens waarop de bepalingen inzake bescherming van het privéleven en van persoonsgegevens van toepassing zijn.

De informatiebeheerder is zich bewust van het feit dat de persoonsgegevens en gevoelige gegevens moeten worden beschermd.

De informatiebeheerder wijst op de risico's eigen aan zijn domein, dringt er bij het bestuur op aan om gepaste instructies te krijgen met betrekking tot die risico's. Hij/zij past technische, procedurele,

communicatieve en organisatorische maatregelen toe waardoor de persoonsgegevens en gevoelige gegevens beveiligd en beschermd zijn tegen elke niet toegelaten gegevensverwerking. De informatiebeheerder houdt naast de risico's, ook rekening met de aard, de omvang, de context en de verwerkingsdoeleinden.

De informatiebeheerder waakt erover dat ook derden en externe medewerkers de bepalingen met betrekking tot de bescherming van persoonsgegevens en gevoelige gegevens naleven.

De informatiebeheerder mag communicatie en toegangen controleren binnen het kader van zijn/haar bevoegdheden en mits de naleving van de wettelijke en reglementaire bepalingen.

De informatiebeheerder gaat ervan uit dat alle informatie van de organisatie vertrouwelijk is en als dusdanig behandeld moet worden, zowel door zichzelf als door alle medewerkers van de organisatie.

Artikel 18 – Informatie- en documentatieplicht

De informatiebeheerder licht alle betrokken medewerkers duidelijk en regelmatig in over hun verantwoordelijkheden bij het toegelaten gebruik van informatiesystemen via bewustmaking, opleiding en evaluaties.

De informatiebeheerder licht naar aanleiding van een interventie zijn/haar handelingen tijdig en op een begrijpelijke manier toe opdat de betrokken medewerker(s) voldoende geïnformeerd zijn over de gevolgen van (het gebruik van) de informatiesystemen.

De informatiebeheerder waakt erover dat er steeds zo goed mogelijk geactualiseerde documentatie voorhanden is waarin het informatiesysteem (zoals ontwikkeling, hard- en software, infrastructuur) op zodanige wijze wordt beschreven dat elke betrokken persoon zich een precies en volledig totaalbeeld zou kunnen vormen. De bedoeling ervan is een continu beheer van het informatiesysteem te garanderen.

De informatiebeheerder kan vragen of problemen bespreken met andere informatiebeheerders en indien nodig ook in vertrouwen bespreken met de dienst informatieveiligheid van de KSZ.

2.3 REGLEMENT GEGEVENSBESCHERMING EN INFORMATIEVEILIGHEID

Artikel 19 – Algemeen

Binnen het lokaal bestuur worden talloze persoonsgegevens verwerkt. De verwerking van persoonsgegevens moet gebeuren overeenkomstig de toepasselijke regelgeving, waaronder de Algemene Verordening Gegevensbescherming en nationale wetgeving.

De medewerking van alle medewerkers is van essentieel belang voor de informatieveiligheid en de privacy van de persoonsgegevens. Wanneer een medewerker bij de uitvoering van de opdracht persoonsgegevens dient te verwerken, neemt hij de in dit reglement beschreven regels en verantwoordelijkheden steeds in acht.

Artikel 20 – Algemene principes voor een correcte verwerking

RECHTMATIGHEID

Medewerkers van het bestuur verwerken persoonsgegevens op een rechtmatige wijze. De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de onderstaande voorwaarden is voldaan:

- De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij het bestuur partij is
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op het bestuur rust
- De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen
- De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan het bestuur is opgedragen

Indien een verwerking gebeurt op grond van de toestemming van de betrokkene, zorgt de medewerker ervoor dat de voorwaarden daaromtrent uit de Wetgeving Gegevensbescherming zijn vervuld. Deze vereist dat de toestemming gebeurt door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, elektronisch aanvinken, of een mondelinge verklaring waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt. Er moet in ieder geval kunnen worden aangetoond dat de betrokkene, op actieve wijze, heeft toegestemd. Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit gelden niet als toestemming.

De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend.

De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken voor toekomstige verwerkingen.

GERECHTVAARDIGDE DOELEINDEN

Persoonsgegeven moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet voor andere doeleinden gebruikt worden.

MINIMALE GEGEVENSVERWERKING

Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt zijn tot wat noodzakelijk is.

JUISTHEID

De persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd.

OPSLAGBEPERKING

De persoonsgegevens worden bewaard conform de archiefwetgeving.

INTEGRITEIT EN VERTROUWELIJKHEID

Persoonsgegevens moeten beschermd worden tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Artikel 21 – Toegang tot dossiers/bestanden met persoonsgegevens

De medewerkers die daartoe – uit hoofde van hun beroep – gemachtigd zijn, hebben slechts inzage in een dossier met persoonsgegevens en mogen slechts kennisnemen van de inhoud van het dossier voor zover dat noodzakelijk is voor de uitoefening van hun beroepswerkzaamheden. Zij nemen daarbij enkel kennis van die gegevens die noodzakelijk zijn voor de uitoefening van hun beroepswerkzaamheden. Dit geldt voor alle bestanden waarin persoonsgegevens worden verwerkt.

Wanneer een medewerkers vaststelt dat een andere medewerker zicht toegang heeft verschaft tot een bestand met persoonsgegevens zonder daartoe bevoegd te zijn, wordt dit gemeld aan de dienstverantwoordelijke.
De medewerker deelt geen persoonsgegevens en/of informatie met anderen indien zij geen rechtmatige ontvanger zijn.

Artikel 22 – Geen verwerking voor eigen doeleinden

De medewerker zal de persoonsgegevens niet voor eigen doeleinden of die van derden verwerken, noch de persoonsgegevens aan derden verstrekken, noch deze doorsturen naar een lang geleden buiten de Europese Unie zonder daartoe een schriftelijk instructie te hebben ontvangen van het bestuur.

Artikel 23 – Bijstand verlenen aan de uitvoering van de verplichtingen van het bestuur

Iedere medewerker verleent bijstand aan het bestuur in de verantwoordelijkheid van het bestuur om haar verplichtingen in het kader van gegevensbescherming na te leven. Hieromtrent moeten medewerkers:

- Melding maken van risico's, incidenten, ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen. Alle meldingen moeten zo snel mogelijk gemeld worden via C-Smart, DPO (data protection officer) voor stad/OCMW Bilzen-Hoeselt.
- Melding maken van nieuwe verwerkingen van persoonsgegevens om het register van verwerkingsactiviteiten up to-date te houden.
- Melding maken van nieuwe partners/leveranciers ikv het afsluiten van een contractuele verbintenis (verwerkingsovereenkomst) rond het verwerken van persoonsgegevens
- Melding maken van een nieuwe verwerking die een mogelijks hoog risico inhoudt voor de rechten en vrijheden van medewerkers of burgers zodat er voorafgaande aan de verwerking een risicoanalyse (gegevensbeschermingseffectbeoordeling) uitgevoerd kan worden
- Melding maken van geplande doorgiftes van persoonsgegevens zodat voorafgaan de rechtmatigheid van de doorgifte kan nagegaan worden. Bij eenmalige grote en systematische doorgiftes van persoonsgegevens dient er conform artikel 8 e-govdecreet een protocol afgesloten te worden.

Artikel 24 – Richtlijnen voor de consultatie van vertrouwelijke stromen

Onder vertrouwelijke stromen verstaan we onder andere KSZ, rijksregister, strafregister, omgevingsvergunningen,…

- Medewerkers die gebruik maken van de vertrouwelijke stromen mogen enkel de persoonsgegevens inzamelen die ze nodig hebben voor de uitoefening van hun functie

- Medewerkers zijn ertoe gehouden maatregelen te treffen om het vertrouwelijk karakter van de gegevens te verzekeren en om ervoor te zorgen dat ze uitsluitend worden aangewend voor professionele doeleinden en voor het vervullen van hun wettelijke verplichtingen
- Iedere opvraging via het netwerk van de KSZ, het rijksregister, het strafregister, wordt gelogd. Bijgevolg zal er regelmatig gecontroleerd worden welke medewerker binnen het bestuur welke opvraging heeft gedaan. Ook de burger kan nagaan wie zijn gegevens heeft geconsulteerd.
- Het consulteren van het rijksregister of andere stromen om bijvoorbeeld het adres van een oude schoolvriend te achterhalen, of de verjaardag van een collega op te zoeken, is totaal onaanvaardbaar en wordt gesanctioneerd
- Medewerkers moeten de reglementen van de portalen (rijksregister, strafregister, KSZ) actief lezen en toepassen

Medewerkers, die zich in de functie van hun taakuitoefening moeten begeven in de ruimtes waarin zich te beveiligen gegevens van persoonlijke aard bevinden, verbinden zich tot geheimhouding.

Indien je niet geautoriseerd bent om kennis te hebben van of toegang te hebben tot persoonlijke gegevens van dossiers betreffende individuele dienstverlening van stad/OCMW tracht je jezelf nooit die toegang te verschaffen. Indien je ongewild wel in aanraking komt met deze gegevens, hetzij op fysieke wijze, hetzij elektronisch of allebei, verbind je je tot strikte geheimhouding.

Wie uit hoofde van zijn functie wel toegang heeft tot genoemde gegevens, hetzij op fysieke wijze, hetzij elektronisch of allebei, hanteert een strikte geheimhoudingsplicht ten aanzien van deze gegevens en onderschrijft de naleving van de minimale veiligheidsnormen waarvan je in kennis gesteld wordt.

Alle medewerkers moeten zich houden aan de gedragscode voor informatiebeheerders binnen het netwerk van de sociale zekerheid.

Artikel 25 – Toegang tot gebouwen

Medewerkers krijgen enkel toegang tot de locaties die zij nodig hebben in het kader van de uitoefening van hun functie. Het gebruik van de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van het lokaal bestuur is enkel toegestaan voor het doel waarvoor deze aan de medewerker ter beschikking zijn gesteld. Onbevoegden toegang verschaffen tot de gebouwen van het bestuur is verboden.

De voor de medewerker bestemde toegangsmiddelen mogen niet gekopieerd of gedeeld worden met collega's of derden. Bij vermissing, ontvreemding, misbruik of ander onrechtmatig gebruik van de verstrekte toegangspas, sleutels, tags, toegangscodes, apparatuur of software stelt de medewerker onmiddellijk de daartoe aangewezen personen binnen het lokaal bestuur hiervan in kennis.