INFORMATIEVEILIGHEID- EN GEGEVENSBESCHERMINGSBELEID

INFORMATIEVEILIGHEID EN GDPR-TOEPASSING BINNEN LOKAAL BESTUUR RANST

Abstract

Versie

VERSIE	DATUM
1.0	Mei 2020
2.0	Juni 2025

Verantwoordelijken

	NAAM	FUNCTIE	HANDTEKENING EN DATUM
GESCHREVEN DOOR	KINA	DPO	
HERZIEN DOOR	Karen Verheyen	DPO	
GOEDGEKEURD DOOR			

Aanpassingsgeschiedenis

DATUM	REDEN VOOR AANPASSING	AUTEUR	VERSIE
06/06/2025	Nieuw legislatuur	Karen Verheyen	2.0

INHOUDSOPGAVE

INTRODUCTIE

Informatie is een van de belangrijkste bezittingen binnen een lokaal bestuur en zit bovendien verspreid doorheen de gehele organisatie. Informatie an sich en de verwerking ervan heeft de afgelopen jaren een enorme sprong gemaakt, gezien de digitalisering en automatisering van de systemen. Een gevolg hiervan is het ontstaan van nieuwe risico's en uitdagingen waarmee alle organisaties geconfronteerd worden. In het licht hiervan zijn ook nieuwe regels ontstaan die de aandacht voor het veiligstellen van persoonsgegevens wil vergroten. Zo is op 25 mei 2018 de GDPR (General Data Protection Regulation) of AVG (Algemene Verordening Gegevensbescherming) in voege getreden. De GDPR bevestigt enkele bestaande principes, maar introduceert ook enkele nieuwe accenten. Door middel van een systeem op te zetten rond informatieveiligheid kan er tegemoet gekomen worden aan de principes die centraal gesteld worden.

1. WAAROM DIT BELEID? (MISSIE)

Het informatieveiligheidsbeleid is opgesteld om te helpen bij het beheren van (persoonlijke) data in de context van de dagelijkse activiteiten van lokaal bestuur Ranst, om zo tegemoet te komen aan enerzijds de principes van **informatieveiligheid** en anderzijds de regels opgelegd door de Algemene Verordening Gegevensbescherming (**AVG**) of General Data Protection Regulation (**GDPR**). Deze gids geeft met andere woorden aan hoe er binnen lokaal bestuur Ranst omgegaan wordt met allerlei data en persoonsgegevens.

2. WAT WILLEN WE BEREIKEN? (VISIE)

Het informatieveiligheidsbeleid en de maatregelen die hieruit voortvloeien is primair gericht op de bescherming van de informatie die lokaal bestuur Ranst in bezit heeft. De focus is gericht op informatie(uitwisseling) in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over ICT of het bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.).

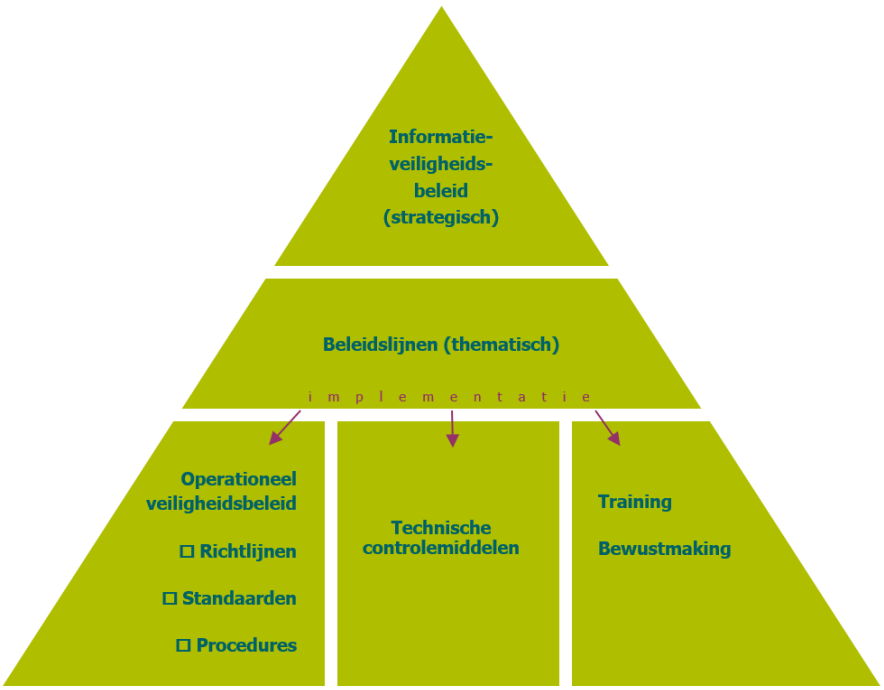
Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeentelijke organisatie en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

3. ALGEMEEN

3.1. SITUERING

Dit document omvat een brede, strategische kijk op informatieveiligheid binnen lokaal bestuur Ranst.

Het informatieveiligheidsbeleid kadert zich binnen de uitbouw van een Information Security Management System (ISMS). Dit systeem zorgt er voor dat er voldoende aandacht gaat naar (persoons)gegevens en mogelijke schendingen van bepaalde principes of rechten voorkomen wordt. Het informatieveiligheidsbeleid heeft betrekking op alle elementen uit het gelaagd model, onderstaand grafisch weergeven in piramidevorm (zie figuur 1).



Figuur 1: Gelaagd model van informatieveiligheid

3.2. TOEPASSINGSGEBIED

Het informatieveiligheidsbeleid is van toepassing op alle informatie en informatiesystemen die lokaal bestuur Ranst in bezit heeft.

3.3. WETTELIJK KADER

Op het moment dat dit document opgesteld is, is volgende wet- en regelgeving van toepassing:

- Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen
- Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid
- Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (e-govdecreet)
- Besluit van de Vlaamse Regering van 15 mei 2009 houdende de uitvoering van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer
- Algemene Verordening Gegevensbescherming (AVG), 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
- Decreet van 22 december 2017 over het lokaal bestuur.
- 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 (AVG-decreet)
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens
- Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische gegevensverkeer.

- Decreet van 7 december 2018 (Bestuursdecreet)
- De wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid (de "NIS2-wet") zet Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 (de "NIS2-richtlijn") om in België.
- De verordening (EU) 2024/1689 tot vaststelling van geharmoniseerde regels inzake artificiële intelligentie (AI-act)
- Het koninklijk besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Richtlijnen

- Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens in steden en gemeenten, in instellingen die deel uitmaken van het netwerk dat beheerd wordt door de kruispuntbank van de sociale zekerheid en bij de integratie OCMW – gemeente. Versie 3.0 - december 2015
- Minimale normen informatieveiligheid en privacy, versie 2017
- CCB richtlijn n° 1/2024 voor de verschillende informatiesystemen van de administraties en publieke instellingen.

3.4. DOELGROEP

Dit document dient gehandhaafd te worden door:

- ☐ Iedere werknemer van Lokaal Bestuur Ranst
- ☐ Iedere contractant, leverancier of derde die toegang krijgt tot de informatie en informatiesystemen die Lokaal Bestuur Ranst aanlevert
- ☐ Iedere subafdeling van het lokaal bestuur

4. WAT IS INFORMATIEVEILIGHEID VERSUS GDPR?

4.1. WAT IS INFORMATIEVEILIGHEID?

Informatieveiligheid heeft betrekking op het beschermen van de informatie tegen allerlei bedreigingen die een schending kunnen veroorzaken van (één van) de volgende principes of betrouwbaarheidseisen:

1. **Vertrouwelijkheid**: Enkel gerechtigden hebben toegang tot bepaalde persoonsgegevens.
2. **Integriteit**: De data mag niet onterecht gewijzigd of gewist worden.
3. **Beschikbaarheid**: Informatiesysteem is beschikbaar op moment dat organisatie het nodig heeft.

Het nemen van enkele maatregelen, op basis van de verbonden risico's, kan ervoor zorgen dat bovenstaande principes gewaarborgd worden en bovendien een goede werking van de organisatie verzekerd wordt. Onvoldoende informatieveiligheid kan ervoor zorgen dat de betrouwbaarheidseisen geschonden worden.

4.2. WAT IS GENERAL DATA PROTECTION REGULATION (GDPR)?

Daarnaast is op 25 mei 2018 ook de GDPR/AVG van kracht gegaan en dienen de lokale besturen compliant te zijn met deze regelgeving. Specifiek in het kader van GDPR dient er omschreven te worden hoe er **binnen de organisatie** omgegaan wordt met specifiek **persoonsgegevens**.

Vooraleer nader bepaald kan worden hoe men binnen de organisatie om gaat met persoonsgegevens, is het van belang om te weten welke specifieke betekenissen kunnen worden gegeven aan bepaalde begrippen binnen de context van databeveiliging, met andere woorden over *wat* het gaat.

TERM	BETEKENIS
Persoonsgegevens	Alle informatie die direct of indirect gerelateerd is aan een geïdentificeerd of identificeerbaar datasubject.
Datasubject	Elke natuurlijke persoon van wie de persoonsgegevens verwerkt wordt door een verwerkingsverantwoordelijke of een verwerker.
Verwerking	Elke bewerking op persoonlijke gegevens, zelfs het openen ervan op een scherm, wordt beschouwd als 'verwerken'. Bedenk dat wanneer u persoonsgegevens op welke manier dan ook gebruikt of benadert, dit wordt beschouwd als 'verwerking'.
Verwerkings-verantwoordelijke	De entiteit die verantwoordelijk is voor de persoonsgegevens, die beslist waarvoor de persoonsgegevens moet worden gebruikt (doeleinden) en hoe deze zal worden behandeld (de wijze van verwerking). Meestal zal het lokaal bestuur optreden als verwerkingsverantwoordelijke en bepalen wat, hoe en waarom persoonsgegevens verwerkt worden. Dit is bijvoorbeeld het geval bij het verwerken van personeelsgegevens, het uitvoeren van klantadministratie of leveranciersbeheer.
Verwerker	Een verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke.
Toestemming van het datasubject	Het datasubject moet vrij akkoord gaan met de verwerking van zijn persoonsgegevens en voldoende informatie krijgen over deze verwerking.
Gevoelige data	Persoonlijke gegevens waaruit de raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen, of lidmaatschap van de vakbond, genetische gegevens, biometrische gegevens voor het uniek identificeren van een natuurlijke persoon, gezondheidsgegevens en gegevens betreffende het seksuele leven of seksuele geaardheid van een natuurlijke persoon blijken. Let op: Verwerking van deze data zijn in principe verboden. Hier zijn enkele uitzonderingen op.

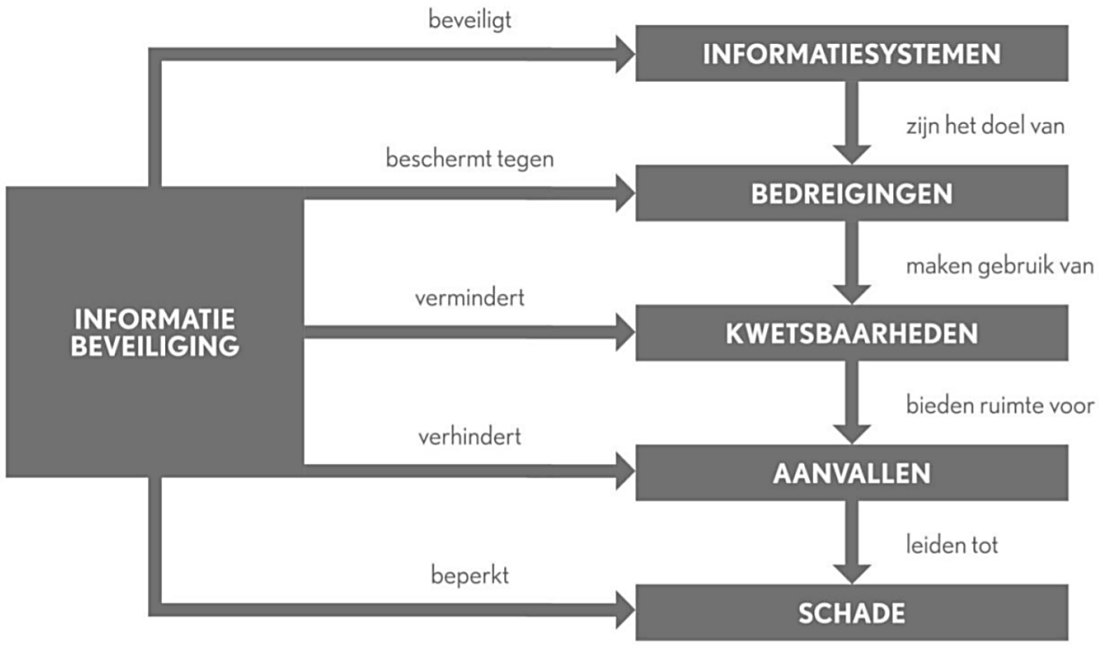
Juridische data	Gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.
Datalek	Persoonlijke data is op de een of andere manier gecompromitteerd (vernietigd, zoekgeraakt, gewijzigd, geopend zonder toestemming ...); er moeten corrigerende maatregelen worden genomen.
Maturiteit	het niveau dat het bestuur compliant is met de AVG-wetgeving en/of algemene richtsnoeren KSZ
Risicoanalyse	Inventarisatie van kwetsbaarheden van de werkprocessen en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie.
VTC (Vlaamse Toezichtcommissie)	De Vlaamse handhavingsinstantie die verantwoordelijk is voor het toezicht op de toepassing van de AVG door Vlaamse bestuursinstanties.
GBA (gegevensbescherm ingsautoriteit)	De nationale handhavingsinstantie die verantwoordelijk is voor het toezicht op de toepassing van de AVG. Sinds 25 mei 2018 is de GBA als onafhankelijk controleorgaan ingesteld bij de Kamer van volksvertegenwoordigers. België: Gegevensbeschermingsautoriteit (GBA) Drukpersstraat 35, 1000 Brussel e-mail: contact@apd-gba.be website: www.gegevensbeschermingsautoriteit.be

Ook de principes die voortvloeien uit deze wetgeving, dienen geïntegreerd te worden in het systeem dat opgezet wordt rond informatieveiligheid. In de GDPR worden enkele van de bestaande principes bevestigd (zie bovenstaand), maar worden er ook enkele nieuwe focussen gelegd.

1. **Transparantie**: Persoon dient op de hoogte te zijn dat zijn persoonsgegevens verwerkt wordt. Hij heeft hier zijn toestemming voor gegeven en hij kent zijn rechten.
2. **Doelbeperking**: Persoonsgegevens worden voor een welbepaald doel verzameld en mogen niet voor andere doeleinden worden gebruikt.
3. **Gegevensbeperking**: Enkel de noodzakelijke gegevens voor het beoogde doel mogen worden verzameld (subsidiariteit en proportionaliteit).
4. **Juistheid**: Persoonsgegevens moeten correct zijn en blijven (up-to-date houden). Om dit principe te verzekeren kunnen interne procedures voorzien worden die dit principe waarborgen.
5. **Bewaarbeperking**: Persoonsgegevens mogen niet langer bijgehouden worden dan nodig voor het beoogde doel.
6. **Integriteit en vertrouwelijkheid**: Persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging. Het gebruik van wachtwoorden om ongeautoriseerde toegangen te vermijden, het bijhouden van logs bij wijzigingen aan documenten, enzoverder kunnen hier aan bijdragen.
7. **Verantwoording**: Verantwoordelijken moeten kunnen aantonen dat ze aan de regels van GDPR voldoen.

5. MEERWAARDE VAN INFORMATIEVEILIGHEID/GDPR

Het belang van een structurele uitbouw van informatieveiligheid is om meerdere redenen van belang. Ten eerste heeft de **burger** enkele **verwachtingen** over hoe omgegaan wordt met zijn persoonlijke gegevens. Een lokaal bestuur is immers in het bezit van heel wat (gevoelige) data van een burger, en deze burger verwacht dan ook dat er op een veilige manier omgegaan wordt met deze gegevens en er alles aan gedaan wordt om diefstal of misbruik te voorkomen. Indien bepaalde persoonlijke gegevens niet goed beschermd worden, is er een kans dat er een inbreuk is van de persoonlijke levenssfeer en bovendien het vertrouwen van de burger geschonden is. Om die reden dienen informatiesystemen correct beschermt te worden. Op onderstaand figuur (zie figuur 2) wordt aangegeven dat een correcte informatiebeveiliging zorgt voor een bescherming op meerdere vlakken.



Figuur 2: Belang van informatieveiligheid op meerdere vlakken

Ten tweede kan er niet om heen worden gegaan dat er heel wat **wet- en regelgeving** is dat verplichtingen oplegt. Indien men niet voldoet, kan men in het kader van de GDPR-wetgeving **sancties** opleggen. Het is vooral belangrijk dat je kan aantonen dat je je bewust bent van welke persoonsgegevens je verzameld, in bezit hebt en je actief bezig bent met het veilig stellen van deze persoonsgegevens.

Ten derde kan het **informatieveiligheidsbeleid opgenomen worden in de verwerkingsovereenkomsten en contracten** die aangegaan worden met leveranciers. Er zijn heel wat organisaties die hun beleid mee uitdelen aan leveranciers en op die manier duidelijk maken wat voor hun de spelregels zijn op vlak van informatieveiligheid en het behandelen van persoonsgebonden data. Op die manier moeten de leveranciers ook de kernprincipes die voor het bestuur van belang zijn naleven en respecteren.

Tot slot kan je ook **vragenlijsten** krijgen **van leveranciers**. Hier worden de rollen omgedraaid en vragen grote nutsbedrijven hoe het gesteld is met informatieveiligheid binnen het bestuur. Via een vragenlijst, waarin de GDPR als onderdeel opgenomen is, wordt gepeild naar de maturiteit van het lokaal bestuur.

Kortom is GDPR niet enkel wettelijk verplicht, maar is het ook een kans om je bewust te worden van welke gegevens je organisatie in bezit heeft en hoe omgegaan wordt met deze gegevens. Je kan je afvragen waarom je bepaalde gegevens in bezit hebt, hoe lang je deze bij houdt, welke gevoelige informatie bevat, etc.

6. AANPAK (HOE DOEN WE DIT?)

Uit de missie en visie is reeds duidelijk waarom we dit beleid opmaken en wat we juist willen bereiken. De vraag hierbij is hoe we dit juist gaan doen. In wat volgt worden de kerndoelen die lokaal bestuur Ranst nastreeft toegelicht. Door middel van een risicoanalyse en maturiteitsmeting worden actiepunten bepaald en omgezet in een actieplan. Policies, processen en procedures worden uitgewerkt om medewerkers te helpen bij het veilig omgaan met (persoonlijke) data. Tot slot wordt de organisatorische structuur waarbinnen deze activiteiten zich situeren uitgewerkt.

6.1. CHARTER: KERNDOELEN

Lokaal bestuur Ranst heeft als doel zich conform te stellen met de AVG en de minimale normen informatieveiligheid en privacy.

1. Een duidelijk en helder beleid rond informatieveiligheid en privacy opzetten, valideren, communiceren en onderhouden om de beschikbaarheid, de integriteit en de vertrouwelijkheid te garanderen in lijn met de doelstellingen van de organisatie.
2. Conform de minimale normen informatieveiligheid en privacy en conform alle toepasselijke Belgische en Europese wetten en regelgevingen ageren om verplichtingen na te komen en boetes te vermijden.
3. Formele risico-aanpak rond informatieveiligheid en privacy opzetten, valideren, communiceren en onderhouden om relevante risico's tijdig, consistent en effectief aan te pakken in lijn met de verwachtingen van de organisatie.
4. Duidelijke rollen en verantwoordelijkheden rond informatieveiligheid en privacy van alle betrokken interne en externe personen en organisaties definiëren, valideren, communiceren en opvolgen.
5. De minimale normen informatieveiligheid en privacy omzetten in praktische gedocumenteerde procedures en richtlijnen in functie van de specifieke situatie van de organisatie en gebaseerd op de risicobeoordeling.
6. "Security en Privacy by design" toepassen in de volledige levenscyclus van informatie in de organisatie om betrouwbare, kwalitatieve en efficiënte systemen te ontwikkelen: vanaf de creatie tot de verwijdering of de archivering van informatie.
7. Het niveau van informatieveiligheid en privacy continu verbeteren via een geactualiseerd meerjarenplan en regelmatige sensibiliseringscampagnes naar alle interne en externe betrokken personen en organisaties om zo de kosten van inbreuken te verminderen en om de reputatie en het vertrouwen rond informatieverwerking te behouden.
8. Bij uitbesteding van informatieverwerking aan derde partijen de nodige controlemaatregelen opzetten, valideren, opvolgen en regelmatig controleren omdat de organisatie altijd verantwoordelijk blijft voor de informatieveiligheid en privacy.
9. Regelmatig rapporteren over de stand van informatieveiligheid en privacy om de toepasbaarheid, volledigheid, adequaatheid en effectiviteit van informatieveiligheid en privacy te valideren. Vastgestelde afwijkingen, problemen of incidenten zullen tijdig opgevolgd worden met gepaste acties/sancties in lijn met de interne procedures van de organisatie. Ernstige incidenten of inbreuken in verband met persoonsgegevens worden altijd tijdig geëscaleerd naar de bevoegde instanties.

10. Alle afwijkingen ten opzichte van de minimale normen informatieveiligheid en privacy met een significant risico voorafgaandelijk schriftelijk afstemmen en laten goedkeuren door het Sectoraal Comité van de Sociale Zekerheid

6.2. INFORMATIEVEILIGHEIDSPLAN (ACTIEPLAN)

6.2.1. Risicoanalyse

De aanpak van informatiebeveiliging is 'risk based'. Dit wil zeggen dat maatregelen worden getroffen op basis van een risicoanalyse. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van de werkprocessen en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces of de organisatie (risico = kans x impact).

Per risico zal één van de volgende strategieën gekozen worden om deze te verkleinen:

- Treat the risk (reduceren): verkleinen van het risico door middel van het nemen van informatiebeveiligingsmaatregelen.
- Take the risk (accepteren): het risico is zo klein dat de gevolgen acceptabel zijn.
- Terminate the risk (vermijden): wanneer er een groot risico bestaat voor een bedrijfsactiviteit die weinig tot niets oplevert dan wordt deze bedrijfsactiviteit gestaakt.
- Transfer the risk (overdragen): overhevelen van het risico naar een derde partij door middel van uitbesteding of het afsluiten van verzekeringen.

Vooraleer een actieplan met maatregelen opgemaakt wordt, wordt een risicoanalyse gedaan zodat prioritaire maatregelen genomen kunnen worden. De hoogste risico's worden opgenomen.

6.2.2. Maturiteitsmeting

De maturiteit van het bestuur heeft betrekking op het niveau dat het bestuur compliant is met de GDPR-wetgeving en/of algemene richtsnoeren KSZ. Voor de graad van maturiteit uit te drukken, wordt volgende schaal gehanteerd:

Cijfer	Maturiteitsniveau	Scoring van de naleving van normen
(0)	Onbestaande	De norm wordt totaal niet nageleefd. Er is geen enkele beheersmaatregel betreffende de norm.
(1)	Initieel/Ad-hoc	De norm wordt informeel en ad-hoc nageleefd vanuit een zeker bewustzijn, en als reactie op incidenten. De maatregelen zijn niet gedocumenteerd of gecommuniceerd.
(2)	Herhaalbaar maar intuïtief	De norm wordt meer gestructureerd nageleefd. Er zijn geen detailanalyses die de keuze van de maatregelen onderbouwen. Er is geen controle op de effectiviteit van de maatregelen.
(3)	Gedefinieerd	De norm wordt op een gestructureerde manier nageleefd. De maatregelen zijn gestandaardiseerd, gedocumenteerd, gecommuniceerd en worden

		toegepast. De naleving wordt gecontroleerd, maar dit gebeurt niet gestructureerd.
(4)	Beheerd en meetbaar	De effectiviteit van de maatregelen om de norm na te leven wordt gemeten, en deze input wordt gebruikt om de maatregelen bij te sturen.
(5)	Geoptimaliseerd	Het ISMS is geoptimaliseerd via benchmarking en kwaliteitscertificaten.

6.2.3. Actieplan

Voortvloeiend uit de risicoanalyse en de maturiteitsmeting, wordt het veiligheidsplan opgesteld met actiepunten voor de komende jaren. De nodige maatregelen worden geïdentificeerd om het risiconiveau op een niveau te brengen dat voor de organisatie aanvaardbaar is. Het actieplan bevat met andere woorden de concrete maatregelen die binnen lokaal bestuur Ranst genomen worden. Binnen het actieplan worden de hoogste prioriteiten bepaald.

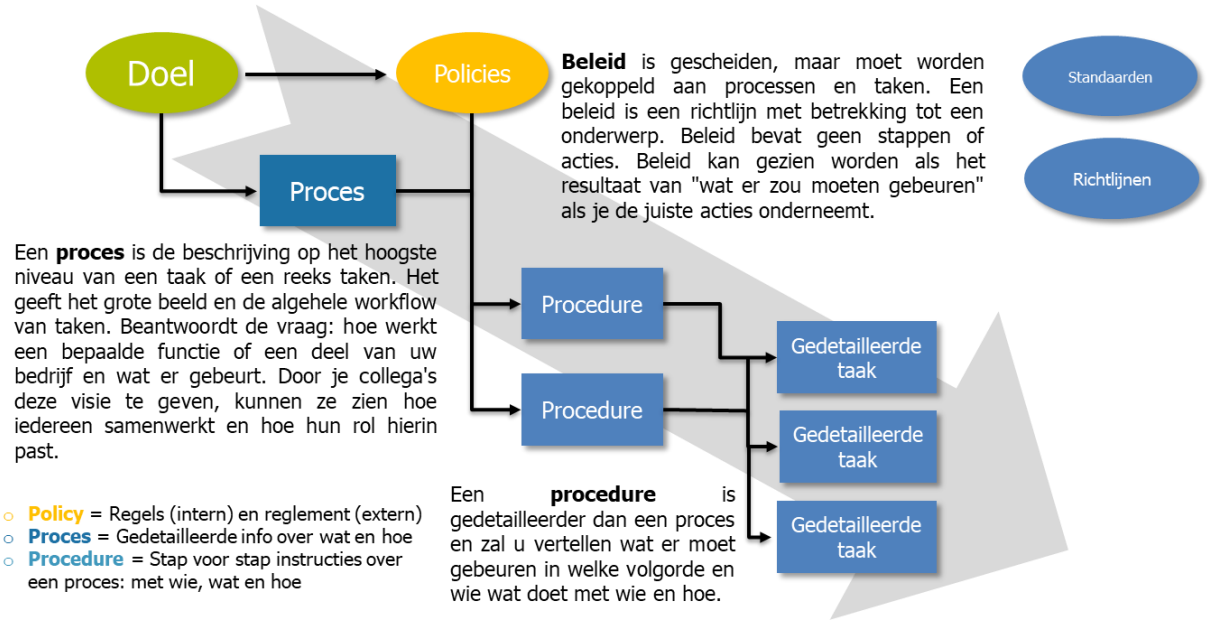
6.2.4. Frequentie van herziening

In onderstaande tabel wordt de frequentie weergeven waarin de risicoanalyse, maturiteitsmeting en het actieplan worden opgesteld.

Activiteit	**Frequentie**
Risicoanalyse	
In samenspraak met IVC + opmaak door DPO	driejaarlijks
Maturiteitsmeting	
In samenspraak met IVC + opmaak door DPO	driejaarlijks
Informatieveiligheidsplan	
In samenspraak met IVC + opmaak door DPO	driejaarlijks
Prioriteiten bepalen met IVC per jaar	jaarlijks
Plan bespreken en zo nodig aanpassen	kwartaal

6.3. POLICIES, PROCESSEN EN PROCEDURES

Binnen lokaal bestuur Ranst wordt het gedrag van de medewerkers in de juiste richting gestuurd door middel van policies (thematische beleidslijnen), processen en procedures (zie ook figuur 3). Deze worden op tactisch en operationeel niveau uitgewerkt, en helpen de medewerkers op de werkvloer om juist te handelen als zij in aanraking komen met persoonsgegevens, hardware, software, datalekken, etc.



Figuur 3: Policies, processen en procedures

6.4. ORGANISATIESTRUCTUUR

De organisatie van het informatieveiligheid- en gegevensbeschermingsbeleid gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Dit hoofdstuk beschrijft hoe het informatieveiligheid- en gegevensbeschermingsbeleid in lokaal bestuur Ranst georganiseerd is. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Rekening houdend met de te hanteren normen op het vlak van informatieveiligheid en de wetgeving omtrent gegevensbescherming stelt lokaal bestuur Ranst vanuit de organisatie brede doelstellingen een integraal beleid rond informatieveiligheid en gegevensbescherming vast. Dit betreft het strategisch niveau (richtinggevend) waarbij de organisatie, alsmede de doelen, bereik en ambitie op het gebied van het informatieveiligheid- en gegevensbeschermingsbeleid aan de orde zijn.

Op tactisch niveau (sturend) wordt het informatieveiligheid- en gegevensbeschermingsbeleid voorts vertaald naar plannen en specifieke beheersmaatregelen zijnde organisatorische-technische richtlijnen.

Op operationeel niveau (uitvoerend) worden de richtlijnen in concrete procedures en werkvoorschriften omschreven.

Voor elk niveau wordt beschreven welke verantwoordelijkheden en taken de verschillende rollen met zich meebrengen.

6.4.1. Richtinggevend

6.4.1.1. VERWERKINGSVERANTWOORDELIJKE

De algemeen directeur is eindverantwoordelijk voor het informatieveiligheid- en gegevensbeschermingsbeleid en stelt het beleid en de basismaatregelen op het gebied van het informatieveiligheid- en gegevensbeschermingsbeleid vast.

De toepassing en werking van het informatieveiligheid-en gegevensbeschermingsbeleid wordt op basis van regelmatige rapportages geëvalueerd.

6.4.1.2. INFORMATIEVEILIGHEIDSCEL (IVC)

Om de lopende zaken omtrent informatieveiligheid en AVG te bespreken, is er een informatieveiligheidscel (IVC) opgericht die ongeveer 4x per jaar samen komt. Onder andere het informatieveiligheidsbeleid, informatieveiligheidsplan, prioriteiten en dergelijke wordt binnen deze cel besproken.

Binnen lokaal bestuur Ranst zijn volgende personen lid van de IVC:

Naam	**Functie**
Wim Van der Schoot	Algemeen directeur
Maarten Vanachter en Koen Bosmans	ICT coördinator
Karen Verheyen	Data Protection Officer (DPO)
Alix Lorquet	Adviseur interne en juridische zaken
Elien Schuerwegen	Beleidsmedewerker sociale zaken

6.4.2. Sturend

6.4.2.1. DATA PROTECTION OFFICER (DPO)

Op grond van artikel 37 van de Algemene Verordening Gegevensbescherming (AVG) zijn verwerkingsverantwoordelijken en verwerkers in bepaalde gevallen verplicht een functionaris voor gegevensbescherming of Data Protection Officer (DPO) aan te wijzen. Lokale besturen vallen onder deze verplichting.

Lokaal bestuur Ranst doet beroep op KINA p.v. om gebruik te maken van haar diensten in het kader van informatieveiligheid. KINA p.v. stelt een DPO aan die als externe medewerker de opdrachten zal vervullen.

Het volledige takenpakket die de DPO dient uit te voeren, staat omschreven in het besluit van de Vlaamse Regering betreffende de functionarissen voor gegevensbescherming[1]. De taak van de DPO bestaat onder meer uit:

- Alle medewerkers informeren en adviseren over hun verplichtingen vanuit de AVG en de Kaderwet;

[1] Zie bijlage 1: Besluit van de Vlaamse Regering betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische gegevensverkeer.

- Medewerkers opleiden en hulpmiddelen verstrekken zodanig dat ze binnen de voorziening het informatieveiligheid- en gegevensbeschermingsbeleid kunnen ondersteunen;
- Desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling;
- Met de toezichthoudende autoriteit samenwerken en optreden als contactpunt voor deze autoriteit.
- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- De uniformiteit bewaken;
- Meewerken aan de bewustmaking en opleiding van het personeel;
- Het aanspreekpunt zijn voor incidenten op het gebied van het informatieveiligheid- en gegevensbeschermingsbeleid;
- De verdere afhandeling van incidenten coördineren.
- …

De DPO zal zijn functie onafhankelijk uitvoeren. Om die reden zijn volgende uitgangspunten van toepassing:

- De functionaris ontvangt geen instructies hoe hij/zij zijn taken moet uitvoeren;
- De functionaris kan niet ontslagen of gestraft worden voor de uitvoering van zijn/haar taken;
- Er mag geen belangenvermenging zijn tussen de functionaris-taken en de eventuele andere taken of functies van de functionaris.

6.4.3. Uitvoerend

6.4.3.1. LEIDINGGEVENDE

Naleving van het informatieveiligheid- en gegevensbeschermingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het informatieveiligheid- en gegevensbeschermingsbeleid;
- toe te zien op de naleving van het informatieveiligheid- en gegevensbeschermingsbeleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp informatieveiligheid en gegevensbescherming onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde onderwerpen van het informatieveiligheid- en gegevensbeschermingsbeleid.

De leidinggevende kan in zijn taak ondersteund worden door de Data Protection Officer (DPO).

6.4.3.2. ICT-COÖRDINATOR

De ICT-coördinator vormt een technisch aanspreekpunt inzake informatieveiligheid voor de directie en de medewerkers, en zorgt in de praktijk voor de implementatie van toegangsrechten en de rapportage aangaande digitale informatieveiligheid.

6.4.3.3. MEDEWERKER

Alle medewerkers hebben een verantwoordelijkheid met betrekking tot informatieveiligheid in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het privacyreglement en eraan toegevoegde nota's en visieteksten aangaande het informatieveiligheid- en gegevensbeschermingsbeleid op Lokaal Bestuur Ranst. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists, formulieren en praktische tools.

Medewerkers worden gevraagd om actief betrokken te zijn bij het informatieveiligheid- en gegevensbeschermingsbeleid. Dit kan door meldingen te maken van veiligheidsincidenten, het doen van voorstellen ter verbetering van het informatieveiligheid- en gegevensbeschermingsbeleid en het

uitoefenen van invloed op het beleid. Zelf hebben zij ook een voorbeeldfunctie naar andere medewerkers, externen en vooral cliënten toe.

Medewerkers (ook extern) van Lokaal Bestuur Ranst die toegang kunnen hebben tot persoonsgegevens, zijn gebonden aan een discretieplicht. Welbepaalde (externe) medewerkers zijn wettelijk gebonden aan een beroepsgeheim.

7. INWERKINGTREDING

Het informatieveiligheid- en gegevensbeschermingsbeleid treedt in werking op de dag van zijn goedkeuring door de gemeenteraad van Lokaal Bestuur Ranst. Het beleid wordt periodiek geëvalueerd om rekening te houden met de nieuwe behoeften, de nieuwe praktijken en technieken, de nieuwe bedreigingen en gelopen risico's. Elke wijziging van dit beleid moet door de gemeenteraad worden goedgekeurd. De gemeenteraad zal jaarlijks een verslag krijgen van de stand van zaken.