Informatieveiligheid

Als Stad Turnhout verwerken we een aanzienlijke hoeveelheid informatie, inclusief persoonsgegevens van burgers, medewerkers en derden. Met deze verantwoordelijkheid komt de plicht om zorgvuldig en veilig om te gaan met deze gegevens. Het is essentieel dat we allen, in onze diverse rollen, correct handelen en ons bewust zijn van de risico's die gepaard gaan met de verwerking van deze informatie.

In dit document vind je cruciale inzichten over privacy, de Algemene Verordening Gegevensbescherming (GDPR) en hoe we deze principes in de praktijk kunnen brengen. Door je kennis te verrijken, draag je bij aan onze gezamenlijke inspanningen om de privacy van iedereen te waarborgen en een veilige informatieomgeving te creëren.

Heb je na het lezen van deze pagina nog vragen of wil je meer informatie over hoe om te gaan met persoonsgegevens, privacy of de GDPR? Onze Data Protection Officer (DPO), Nordwin Laeveren van C-smart, staat klaar om je te helpen.

Je kunt vragen, incidenten of problemen eenvoudig aangeven door een melding aan te maken in het MIPS-systeem voor informatieveiligheid. Voor dringende zaken kan je Nordwin ook telefonisch contacteren op het nummer +32 471 88 63 80.

De medewerkers van Strategie & Beleid volgen de samenwerking met C-smart op. Loopt de afwikkeling van een vraag niet zoals gepland of krijg je geen sluitend antwoord, neem dan contact op met Joris Van Gool.

Hieronder vind je een inhoudstabel die verwijst naar belangrijke onderwerpen binnen informatieveiligheid. Ze geven je belangrijke informatie en handige tips. Neem de tijd om elk van deze onderwerpen te verkennen en maak jezelf vertrouwd met onze praktijken en procedures.

Wat is informatieveiligheid ?

In het kort:

Informatieveiligheid houdt in dat informatie wordt beschermd tegen ongeoorloofde toegang, wijziging, verlies of vernietiging. Hierdoor blijven de privacy, integriteit en beschikbaarheid van gegevens gewaarborgd.

Definitie

Informatieveiligheid draait om het beschermen van informatie. Het omvat een reeks maatregelen, procedures en processen die een organisatie toepast om te zorgen voor de beschikbaarheid, vertrouwelijkheid en integriteit van alle soorten informatie. Dit geldt voor informatie opgeslagen op digitale media en in papieren dossiers.

Beschikbaarheid zorgt ervoor dat geautoriseerd personeel op de juiste momenten snel toegang heeft tot informatie en de systemen waarop deze is opgeslagen. Integriteit richt zich op het behouden van de correctheid en consistentie van data, en het voorkomen van onbedoelde wijzigingen. Vertrouwelijkheid garandeert dat alleen bevoegde personen toegang hebben tot bepaalde informatie.

Waarom informatieveiligheid?

Door in te zetten op Informatieveiligheid waarborg je de continuïteit van de organisatie en de dagelijkse werking. We streven ernaar om risico's zoals ongeautoriseerde toegang of misbruik van onze informatie te minimaliseren. Het is cruciaal voor de bescherming van gegevens en het behouden van vertrouwen bij onze burgers. Door risico's zoals cyberaanvallen en datalekken af te zwakken, verzekeren we de veiligheid van persoonsgegevens. Dit versterkt op zijn beurt de band tussen bestuur en gemeenschap, wat onmisbaar is voor onze dienstverlening. Nalatigheid in de omgang met persoonsgegevens kan resulteren in ernstige datalekken, schade aan onze reputatie en wettelijke consequenties.

Hoe informatie veilig houden ?

Informatieveiligheid heeft invloed op elke afdeling binnen onze stad die met persoonsgegevens werkt. Een effectieve bescherming van deze gegevens vereist de samenwerking van verschillende afdelingen om zowel technische als organisatorische maatregelen te integreren. Voor de implementatie van technische beveiligingsmaatregelen speelt onze ICT-dienst een cruciale rol. Organisatorische maatregelen, die een breder bereik binnen onze organisatie hebben, omvatten beleidsontwikkeling en bewustwording. Samen vormen ze de basis van onze informatieveiligheidsstrategie, met een belangrijke rol voor elke dienst in het beschermen van gegevens en het behouden van vertrouwen. Dit samenwerkingsproces omvat het maken van duidelijke afspraken en het waarborgen van processen, ondersteund door passende software, om de risico's te minimaliseren.

Waarop baseren we ons?

Voor het treffen van de nodige beveiligingsmaatregelen baseren we ons op de bestaande wetgeving.

- AVG/GDPR
- Privacywetgeving
- Camera-wetgeving
- Koninklijk besluit van 16 juli 1992 betreffende de bevolkingsregisters en het vreemdelingenregister.
- Decreet lokaal bestuur
- …

De privacywet/GDPR/AVG

In het kort:

Privacy is het recht van een individu om controle te hebben over zijn of haar persoonlijke informatie en hoe deze wordt verzameld, gebruikt en gedeeld.

Om de privacy te garanderen is er de ‘Algemene verordening gegevensbescherming (AVG)’ of ‘General Data Protection Regulation (GDPR)’. Dit is een Europese verordening die de regels voor de verwerking van persoonsgegevens door bedrijven en overheidsinstanties vastlegt en standaardiseert in de hele Europees Economische Ruimte. Als lokaal bestuur moeten we deze regels volgen.

Privacy

Privacy wordt vaak omschreven als 'het recht om met rust gelaten te worden'. In de context van de hedendaagse digitale wereld refereert privacy veelal aan data privacy, ofwel het recht om zelf te bepalen welke persoonlijke informatie je deelt en met wie. Sommige informatie wil je bijvoorbeeld wel met vrienden delen, maar niet met anderen. In een tijdperk waarin communicatietechnologieën alomtegenwoordig zijn, is de kans op zowel het gebruik als misbruik van persoonlijke gegevens aanzienlijk toegenomen. Door je privacy actief te beschermen, kun je ervoor zorgen dat bepaalde aspecten van je leven afgeschermd blijven voor de buitenwereld.

GDPR / AVG

De Algemene Verordening Gegevensbescherming (AVG), internationaal bekend als GDPR, markeert een belangrijke mijlpaal in de bescherming van persoonsgegevens binnen de Europese Unie. Voor lokale besturen betekent dit een verhoogde verantwoordelijkheid in hoe zij omgaan met de gegevens van burgers. De verordening eist dat deze organisaties zorgvuldig omgaan met het verzamelen, verwerken en bewaren van persoonlijke informatie, maar ook dat zij de privacyrechten van individuen respecteren. Dit omvat het waarborgen van transparantie over gegevensverwerking, het verstrekken van duidelijke informatie over hoe gegevens worden gebruikt, en het bieden van mogelijkheden aan burgers om hun gegevens in te zien, te corrigeren of te verwijderen. De naleving van de AVG is cruciaal, het zorgt niet alleen voor de bescherming van de privacy van burgers, maar versterkt ook het vertrouwen in de lokale overheid als betrouwbare beheerder van persoonlijke informatie.

De AVG, die op 25 mei 2018 van kracht werd, heeft de eerdere nationale privacywetten, waaronder de Belgische Privacywet van 8 december 1992, vervangen.

Wat zijn persoonsgegevens ?

Persoonsgegevens zijn alle informatie die direct of indirect gebruikt kan worden om een persoon te identificeren. Naast de voor de hand liggende voorbeelden zoals naam, adres, e-mailadres en telefoonnummer, zijn er ook minder voor de hand liggende of eigenaardige voorbeelden die onder de definitie van persoonsgegevens vallen. Hier zijn enkele interessante voorbeelden:

- IP-adressen: Een IP-adres kan worden gebruikt om een individuele computer of apparaat op het internet te identificeren, wat indirect kan leiden tot de identificatie van de gebruiker.
- Cookie-ID's: Deze unieke codes worden gebruikt om het gedrag van gebruikers op websites te volgen en kunnen helpen bij het identificeren van een individu.
- Locatiegegevens: Informatie verzameld via GPS of andere middelen die de specifieke locatie van een persoon kunnen onthullen.
- Internetzoekgeschiedenis: De zoekopdrachten die iemand uitvoert, kunnen persoonlijke voorkeuren, interesses of zelfs de locatie onthullen.

Deze voorbeelden tonen aan dat persoonsgegevens een breed scala aan informatie kunnen omvatten, niet alleen de basisidentificatiegegevens. Onder de AVG/GDPR is het essentieel dat organisaties zorgvuldig omgaan met al deze soorten gegevens om de privacy en bescherming van individuen te waarborgen.

Wat zijn verwerkingen van persoonsgegevens ?

‘Verwerking’ omvat alle handelingen met betrekking tot persoonsgegevens, zoals het verzamelen, opslaan, doorsturen, kopiëren, bewerken, verwijderen, enzovoort. Organisaties die persoonlijke informatie beheren, dienen zich aan de privacywetgeving te houden. Deze organisaties, bekend als de 'verwerkingsverantwoordelijken', zijn aansprakelijk voor het correcte beheer van de gegevens die ze verzamelen. Het is essentieel dat elke organisatie die persoonsgegevens verwerkt duidelijk kan maken op welke wijze en met welk doel dit gebeurt, waarbij de naleving van de wettelijke voorschriften gewaarborgd moet zijn.

Wanneer mogen organisaties persoonsgegevens verwerken ?

Je mag als organisatie niet zomaar persoonsgegevens gebruiken. Je moet een aantal regels volgen.

- Je moet een duidelijk en specifiek doel hebben om gegevens op te vragen.
- Je mag enkel die gegevens vragen die ze nodig hebben.
- Je mag gegevens slechts voor een beperkte duur bijhouden.

Daarnaast mag de verwerking enkel gebeuren wanneer aan één van de volgende voorwaarden is voldaan.

- Je hebt toestemming gevraagd aan de betrokkene.
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst. Bijvoorbeeld:
    - arbeidsovereenkomst
- Het gaat om een wettelijke verplichting. Enkele voorbeelden:
    - de foto op onze identiteitskaart en/of rijbewijs (voor herkenning);
    - de bodyscan op de luchthaven (voor de veiligheid);
    - het delen van onze bloedgroep aan de dokter vlak voor een operatie (voor de gezondheid);
- Het is noodzakelijk om een vitaal belang te beschermen, vaak gezondheid. Bijvoorbeeld:
    - COVID pandemie;
- De verwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak. Bijvoorbeeld:
    - Bewakingscamera’s op de openbare weg.

Let op: gegevens die worden verzameld met toestemming, mag je niet zomaar voor om het even wat gebruiken! Je mag ze enkel gebruiken voor het doel waarvoor ze werden gevraagd.

Incidenten

In het kort:

Alle vastgestelde incidenten en potentiële risico's onmiddellijk intern melden.
Bij kritische incidenten neem je direct telefonisch contact met ICT en de DPO, en informeer je je leidinggevende.

Incidentenprocedure
De regelgeving rond informatieveiligheid vereist dat lokale besturen elk incident met betrekking tot informatieveiligheid en privacy intern melden. Daarnaast zijn ze in bepaalde situaties verplicht om de Gegevensbeschermingsautoriteit binnen 72 uur in te lichten en betrokken burgers te informeren over mogelijke datalekken. Een cruciale GDPR-eis is het implementeren van een incidentenprocedure, die duidelijk maakt hoe en wanneer er over incidenten moet worden gecommuniceerd met betrokkenen, klanten en autoriteiten. Medewerkers spelen een essentiële rol in het opmerken en melden van deze incidenten.

Wanneer je incidenten vaststelt, signaleer dit door een melding aan te maken in het MIPS-systeem voor informatieveiligheid. Wanneer een kritisch incident zich voordoet moet je onmiddellijk telefonisch contact opnemen met ICT en onze DPO. Medewerkers brengen ook steeds hun leidinggevende op de hoogte.

Het is belangrijk dat incidenten worden gemeld zodat er maatregelen kunnen worden genomen om herhaling te vermijden. Alle incidenten worden vertrouwelijk behandeld. Ze worden ook genoteerd in een incidentenregister.

Wat is een incident?
Deze procedure is van toepassing op alle incidenten die een inbreuk vormen op de privacy of informatieveiligheid van persoonsgebonden data die het bestuur verwerkt. Medewerkers moeten zowel incidenten als risico’s melden.

Een incident: is een gebeurtenis die de werking van het openbaar bestuur of de privacy van zijn burgers negatief beïnvloed. Er is schade voor het bestuur of de burger.

Een risico: of een bijna-incident is een gebeurtenis waarbij geen direct zichtbare schade is vast te stellen, maar dat in de toekomst wel incidenten kan veroorzaken.

Onder schade verstaan we hier:

- Operationeel: kan personeel nog werken? Is er schade aan bedrijfsprocessen?
- Financieel: is er een kost verbonden aan de schade?
- Juridisch: worden er juridische stappen genomen?
- Compliancy: werden we op de vingers getikt door een hogere overheid?
- Imago: wordt het bestuur in een slecht daglicht gezet?

Enkele voorbeelden van incidenten en risico’s kan je hieronder terugvinden:

Incidenten of risico’s bij ICT

- Je pc is geïnfecteerd met een virus of malware.
- De stroom is uitgevallen; Brand- of waterschade aan ICT-materiaal.
- De serverruimte is niet afgesloten; Pc’s blijven onvergrendeld aan staan.
- Je bent je usb-stick, smartphone, tablet of laptop verloren.

Incidenten of risico’s bij informatietoegang

- Je mailde per vergissing een lijst met adressen of gevoelige persoonsinformatie door naar een verkeerd adres.
- Iemand zet je onder druk om informatie te delen met hem, waar hij eigenlijk geen recht op heeft.
- Er komen gebruikers zonder de nodige bevoegdheid in aanraking met persoonsgegevens.
- Dossiers blijven liggen op de printers of in openbare ruimtes.

Incidenten of risico’s bij de toegang tot de gebouwen

- De deuren van het gebouw of van bepaalde ruimtes blijven ’s nachts openstaan.
- Je stelt vast dat de alarmcode van het gebouw werd doorgegeven aan een externe.
- Er is een inbraak geweest in een lokaal waar ook gevoelige persoonsinformatie ligt.

Kritische incidenten
Bij een grote impact en hoge urgentie spreken we van een kritisch incident. Vooral de impact op de gebruikers speelt hierbij een belangrijke rol. Enkele voorbeelden:

- Een deel van de datacommunicatie van en naar de gemeente ligt plat door een storing in het netwerk.
- Een belangrijke database blijkt corrupt te zijn.
- Meerdere servers worden geïnfecteerd.
- Persoonsgegevens en vertrouwelijke informatie van burgers worden per ongeluk op een publiek toegankelijk forum geplaatst.

Bij een kritisch incident moet je onmiddellijk telefonisch contact opnemen met ICT en onze DPO. Medewerkers brengen ook steeds hun leidinggevende op de hoogte.

Rechten van betrokkenen

In het kort:

Elke burger kan vragen welke persoonsgegevens we van hem of haar bijhouden en waarom.

Als organisatie zijn we verplicht om hierop te antwoorden.

Welke rechten heeft de betrokkenen ?
De AVG beschermt niet alleen de verwerking van persoonsgegevens, maar kent ook specifieke rechten toe aan de personen wiens gegevens worden verwerkt. Wanneer je als medewerker een aanvraag voor het uitoefenen van deze rechten ontvangt, verwijs je naar formulier op website: https://www.turnhout.be/persoonsgegevens

1. Recht van inzage:

Iedereen heeft het recht om inzage te vragen in de persoonsgegevens die over hem of haar worden bewaard.

2. Recht op correctie:

Wanneer er foutieve informatie wordt verzameld, kan de persoon in kwestie vragen om zijn of haar gegevens te verbeteren.

3. Recht om vergeten te worden:

Iedereen kan vragen om onjuiste of oude gegevens te laten wissen, om welke reden dan ook.

4. Recht op overdracht van gegevens:

Stelt individuen in staat om hun persoonsgegevens van de ene organisatie naar de andere te verplaatsen, te kopiëren of door te geven op een veilige manier, zonder belemmering. Dit versterkt de controle van individuen over hun eigen gegevens door hen de vrijheid te geven deze naar een andere dienstverlener te brengen.

5. Recht om bezwaar in te dienen:

Iedereen kan vragen om zijn of haar gegevens niet meer te gebruiken (tenzij er dwingende redenen zijn om dat wel te doen).

6. Recht om toestemming in te trekken

Iedereen kan op elk moment een eerder gegeven toestemming intrekken en dit zonder verdere uitleg.

7. Beveiliging van de gegevens:

Wie persoonsgegevens verzamelt, is verplicht om deze streng te beveiligen.

Privacyverklaring

In het kort:

Een privacyverklaring informeert individuen over hoe hun persoonsgegevens worden gebruikt en voor welke doeleinden.

Wat is een privacyverklaring?

De GDPR vereist dat organisaties transparant zijn over de verwerking van persoonsgegevens (artikelen 12-14). Een privacyverklaring vervult deze verplichting. Ze maakt duidelijk hoe je gegevens behandelt, met welk doel dat gebeurt en welke rechten individuen hebben als ze het niet eens zijn met de verwerking. Het doel van een privacyverklaring is om de personen die gegevens verstrekken te informeren en hen in staat te stellen geïnformeerde keuzes te maken.

Wat lees je in een privacyverklaring?

In een privacyverklaring moet volgende informatie staan:

- de contactgegevens van de organisatie;
- welke persoonsgegevens worden verwerkt;
- waarom persoonsgegevens worden verzameld;
- of persoonsgegevens worden gedeeld met anderen;
- hoe lang persoonsgegevens worden bijgehouden;
- hoe foutieve persoonsgegevens verbeterd of gewist kunnen worden;
- hoe gegeven toestemmingen ongedaan gemaakt kunnen worden;
- hoe je een klacht kan indienen bij de Gegevensbeschermingsautoriteit.

Onze privacyverklaring vind je terug op de website https://www.turnhout.be/privacyverklaring

Raadplegen gegevens uit het bevolkingsregister

In het kort:

Raadpleging van de registers door medewerkers van een lokaal bestuur is enkel toegestaan voor interne doeleinden en bij uitvoering van een wettelijk of decretaal opgelegde taak

Privégebruik van deze registers door gemeentepersoneel, inclusief ambtenaren en OCMW-medewerkers, is strikt verboden.

Kan informatie die je nodig hebt uit het bevolkingsregister gehaald worden?
De raadpleging van het bevolkingsregister voor privégebruik door medewerkers van de gemeentediensten en het openbaar centrum voor maatschappelijk welzijn is strikt verboden.

Het bevolkingsregister kan wel worden geraadpleegd voor intern gebruik, maar hiervoor gelden bepaalde regels. De raadpleging van het bevolkingsregister door de gemeentelijke diensten en de diensten van het OCMW is slechts toegestaan voor interne doeleinden. Interne doeleinden wil zeggen: de gemeentelijke diensten willen de gegevens raadplegen in het kader van de uitvoering van een hen wettelijk of decretaal opgelegde taak. Gevallen waarbij de gemeentelijke diensten de bevolkingsregisters raadplegen voor duidelijk ‘interne doeleinden’ moeten geen onderwerp uitmaken van een collegebeslissing.

Andere vormen van interne raadpleging:

- De raadpleging van bevolkingsregisters door gemeentebesturen voor specifieke communicatie, zoals het aanschrijven van jubilarissen of nieuwe bewoners, moet onderdeel zijn van een vastgesteld beleid en mag niet op persoonlijk initiatief gebeuren. Hiervoor is een besluit nodig van het college van burgemeester en schepenen. Dat besluit moet gebaseerd zijn op algemeen belang. Het gebruik van persoonsgegevens moet proportioneel zijn, waarbij de voorkeur gaat naar minder privacygevoelige communicatiemethoden. Je moet elke beslissing duidelijk motiveren binnen het kader van het beleid.
- Bevolkingsregisters die meer dan 120 jaar geleden werden afgesloten, kan je vrij raadplegen indien dit gebeurt in het kader van genealogische, historische of andere wetenschappelijk doeleinden.

De personen die de registers willen raadplegen, moeten aantonen dat de raadpleging in het kader van hun opdracht gebeurt.

Bij twijfel, voor hulp of met vragen over dit onderwerp kan je steeds advies vragen aan de DPO via een melding in het MIPS-systeem voor informatieveiligheid.

Verwerkersovereenkomsten/protocollen

In het kort:

Een Verwerkersovereenkomst (VWO) is een contract tussen een verwerkingsverantwoordelijke en een verwerker van persoonsgegevens. Dit contract is verplicht wanneer persoonsgegevens namens de verwerkingsverantwoordelijke worden verwerkt.

Doel

Wanneer Stad Turnhout een externe partij inschakelt om persoonsgegevens te verwerken, is een verwerkersovereenkomst (VWO) noodzakelijk. Bijvoorbeeld, als een IT-bedrijf toegang heeft tot persoonsgegevens voor het onderhoud van systemen, moet er een VWO worden opgesteld. De VWO stelt dan duidelijke eisen aan deze externe verwerkers over hoe zij met deze gegevens moeten omgaan. Dat zorgt er voor dat de verwerking veilig en volgens de privacywetgeving gebeurt. Een VWO legt de rollen, verantwoordelijkheden, en verplichtingen rond de verwerking van persoonsgegevens duidelijk vast, in overeenstemming met de AVG.

Procedure

Er zijn twee mogelijke routes voor het behandelen van een verwerkersovereenkomst (VWO). In beide gevallen moet je de VWO altijd behandelen als garantie dat je aan de privacyregelgeving voldoet.

In de meeste gevallen beschikt de leverancier al over een VWO, omdat zij deze vaak ook voor andere organisaties of lokale besturen nodig hebben. De leverancier kan dan de bestaande VWO aanleveren. Wanneer je een VWO van een leverancier ontvangt, moet je deze via het MIPS-systeem onder informatieveiligheidsmeldingen aan de DPO bezorgen. De DPO controleert de VWO, geeft advies en agendeert de overeenkomst in e-besluit.

Bij kleinere leveranciers bijvoorbeeld kan het voorvallen dat de leverancier geen VWO heeft. In dat geval kan Stad Turnhout zelf een VWO opstellen in samenwerking met de leverancier. Hiervoor moet je een MIPS-melding aanmaken, zodat de DPO op de hoogte is dat er een VWO moet worden opgesteld. De DPO maakt vervolgens de VWO op in samenwerking met de leverancier en agendeert de overeenkomst in e-besluit.

Versturen nieuwsbrieven of andere mailing

In het kort:

Voor het gebruik van contactgegevens is expliciete toestemming nodig.

Het versturen van nieuwsbrieven of andere mailing gebeurt via het bestaande mailsysteem Flexmail.

Persoonsgegevens die met toestemming zijn verzameld, mogen alleen worden gebruikt voor de specifieke doeleinden waarvoor ze zijn gegeven.

Contactgegevens (bv. e-mailadressen) die al in het bezit zijn van het bestuur

Bij het opstarten van nieuwe projecten binnen het bestuur kan de verleiding groot zijn om direct gebruik te maken van bestaande contactgegevens. De privacywetgeving stelt echter duidelijke eisen aan hoe en wanneer je deze gegevens mag gebruiken.

Het algemeen uitgangspunt is dat individuen expliciete toestemming moeten hebben gegeven voor het soort communicatie dat zij ontvangen. Dit betekent dat je contacten die zich bijvoorbeeld hebben aangemeld voor nieuwsbrieven over bibliotheekactiviteiten, niet zomaar mag benaderen voor kinderopvanginitiatieven zonder hun uitdrukkelijke toestemming. Voor vragen over het correct formuleren van toestemmingsverzoeken kun je altijd terecht bij de DPO.

Bij Stad Turnhout sturen we in het geval van een bestaande lijst met contacten die zijn verzameld via diverse kanalen, een eenmalige mail waarbij je expliciet toestemming vraagt voor de onderwerpen waarover zij willen worden benaderd. Deze communicatie verloopt altijd via het vertrouwde mailsysteem Flexmail, dat wordt gebruikt door de communicatiedienst. Dit zorgt ervoor dat we een duidelijk overzicht behouden van de gegeven toestemmingen, in lijn met de eisen van de privacywetgeving.

Toestemming voor gebruik van gegevens

In het kort:

Wanneer er geen andere rechtsgrond is voor het verwerken van gegevens, kunnen we toestemming vragen aan de betrokkene.

Toestemming vereist dat betrokkenen expliciet akkoord gaan met de verwerking van hun persoonsgegevens, waarbij organisaties moeten kunnen bewijzen dat deze toestemming is gegeven.

Wat is toestemming?
Toestemming is elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee iemand door een ondubbelzinnige actieve handeling de verwerking van zijn/haar persoonsgegevens aanvaardt.

- Vrije toestemming: De betrokkene heeft een echte keuze; toestemming is niet onder dwang.
- Specifieke toestemming: Gericht op een duidelijk en precies doel; geen algemene toestemming voor meerdere doelen.
- Geïnformeerde toestemming: De betrokkene is volledig op de hoogte van de gegevensverwerking en begrijpt waarvoor toestemming wordt gegeven.
- Ondubbelzinnige toestemming: De wilsuiting is duidelijk en laat geen ruimte voor twijfel; het is duidelijk dat de betrokkene akkoord gaat.
- Actieve handeling: De toestemming wordt uitgedrukt door een bewuste actie, zoals het aanvinken van een vakje of het ondertekenen van een document.

Voorwaarden toestemming
Een toestemming moet voldoen aan een aantal voorwaarden:

- Je moet als organisatie kunnen aantonen dat iemand zijn toestemming heeft gegeven.
- Als de toestemming een deel is van een ruimere tekst (bv. huishoudelijk reglement) dan moet je in de tekst duidelijk en begrijpelijk aangeven dat je ook toestemming vraagt om gegevens te verwerken. De persoon moet het onderscheid kunnen maken.
- Mensen moeten hun toestemming altijd en gemakkelijk kunnen intrekken.
- Je mag de toestemming niet vastkoppelen aan een overeenkomst als de verwerking van de gegevens niet noodzakelijk is voor de rest van de overeenkomst.
- Bij kinderen onder 16 jaar moet je altijd toestemming van de ouders (of voogd) vragen en je moet moeite doen om aan te tonen dat deze personen effectief het ouderlijk gezag hebben.

Voorbeelden

- Inschrijven voor een nieuwsbrief
- Het gebruik van cookies op een website
- Aanmelden op een openbare wifi
- Het nemen en publiceren van foto’s

Schriftelijke of mondelinge toestemming
Omdat de bewijslast bij het bestuur ligt, vraag je best schriftelijke toestemming. Hoewel schriftelijke toestemming niet verplicht is volgens de wet, is het vanwege die bewijslast sterk aanbevolen. Mondelinge of stilzwijgende toestemming, zoals bij bewust poseren voor een foto, is ook geldig als deze ondubbelzinnig is.

Omdat het moeilijk is om dergelijke toestemming te bewijzen, adviseert het bestuur echter dat je schriftelijke toestemming verkrijgt. Bij overweging van mondelinge toestemming moet zorgvuldig worden beoordeeld hoe groot het risico op privacyinbreuk is en de kans op bezwaren, met een voorkeur voor schriftelijke toestemming voor duidelijkheid en bewijsbaarheid.

Toestemmingsformulier
Schriftelijke toestemming kan worden gegeven via een fysiek document, maar ook elektronisch, bijvoorbeeld via e-mail of door het aanvinken van een vakje in een online formulier, voldoet als geldige vorm van toestemming.

Denk aan het volgende wanneer je toestemming vraagt:

- Informeer zo duidelijk mogelijk wat het doel is waarvoor je gegevens verzamelt.
- Verwijs steeds naar de privacyverklaring van het bestuur. Daarin staan standaard een aantal verplichte vermeldingen waarover je de betrokkene moet informeren.
- Vermeld steeds dat de betrokkene het recht heeft om op elk moment zijn toestemming in te trekken.
- Vul het goedkeuringsvakje niet vooraf in. De betrokkene moet dit zelf kunnen doen (‘opt in’).

- Als je gegevens verzamelt van kinderen jonger dan 13 jaar gaat, zorg je er voor dat de ouders of voogd ondertekenen.

Je mag de toestemming opnemen in een lange tekst zoals een huishoudelijk reglement of een aanmeldingsformulier. Je moet er dan wel op letten dat het voor de persoon duidelijk is dat

- hij toestemming geeft (geen kleine lettertjes);
- de toestemming ook afzonderlijk kan worden gegeven.

Voorbeeld Toestemmingsclausule
Voor het uitwerken van een specifieke toestemmingsclausule kan je steeds terecht bij onze DPO.

Toestemming één doel

- ☐ Ik geef toestemming dat het bestuur mijn persoonlijke gegevens verder verwerkt voor het verzenden van nieuwsbrieven conform de privacyverklaring.

Toestemming meerdere doelen

Ik geef toestemming dat het bestuur mijn persoonlijke gegevens verder verwerkt conform de privacyverklaring voor

- ☐ het verzenden van nieuwsbrieven, waarvoor ik me inschreef;
- ☐ het verzenden van communicatie over thema's die aansluiten bij de inhoud van deze nieuwsbrieven;
- ☐ het verzenden van informatie over alle zaken in het kader van de dienstverlening van ons bestuur.

Het recht op afbeelding

In het kort:

Voor elke menselijke afbeelding moet je toestemming vragen aan de afgebeelde persoon. Maar let op; toestemming om iemand te fotograferen of te filmen wil niet zeggen dat je toestemming hebt om de foto of het filmpje achteraf ook te gebruiken en te verspreiden. Hiervoor is een afzonderlijke toestemming nodig.

Het principe: altijd toestemming vragen

Beelden maken van een persoon is een verwerking van persoonsgegevens. Zodra er sprake is van een verwerking van persoonsgegevens, moet de GDPR worden toegepast. Dat wil zeggen dat iedereen eigenaar is over zijn eigen portret. Concreet betekent dit dat alleen de persoon zelf kan beslissen of van hem een afbeelding mag worden genomen en gebruikt. Je moet daarom de toestemming vragen om een afbeelding te nemen. Eens je die toestemming hebt, wil dit nog niet zeggen dat je de genomen afbeelding mag publiceren of verspreiden. Beide staan los van elkaar. Je moet voor het publiceren of verspreiden apart toestemming vragen.

Gerichte (directe) of niet-gerichte (indirecte) beelden

Er is een uitbreiding op de algemene regels. Zo heb je geen toestemming nodig voor wat men noemt ‘niet-gerichte’ beelden.

Wat nu precies ‘gericht’ en ‘niet-gericht’ is, hangt sterk af van de context en wordt geval per geval bekeken.

Gerichte beelden focussen op individuen of groepen in een specifieke context, zoals geposeerde foto's.



Niet-gerichte beelden daarentegen leggen algemene, spontane situaties vast zonder specifieke personen te benadrukken, zoals sfeerbeelden van evenementen of openbare plaatsen waarbij personen niet het hoofdonderwerp zijn.




Let wel op met het publiceren of verspreiden van deze foto’s wanneer personen herkenbaar zijn. Dan is het vragen van toestemming wel aan te raden.

Openbare evenementen

Informeer bezoekers vooraf dat er foto’s kunnen worden gemaakt. Bv. op de website, in een folder van het evenement, met affiches op het evenement zelf. Als je ‘directe foto’s’ neemt, vraag toestemming.

Wat als iemand géén toestemming geeft?

In het geval dat iemand geen toestemming geeft om herkenbaar in beeld te worden gebracht, moet je hier uiteraard rekening mee houden. Dit kan bv. door middel van het aanbrengen van een bepaald visueel element (sticker, polsband,..) op grotere evenementen.

Publicatie op grote schaal
Als je een foto wil gebruiken op de cover van het gemeentelijk informatieblad, op een affiche of brochure die op grote schaal wordt verspreid, is het aangeraden om bijkomend toestemming te vragen van de betrokkene voor het gebruik van de foto hiervoor.

Of beter, gebruik de beelddatabank. Turnhout beschikt over een beelddatabank van ongeveer 57 000 foto's. Hieruit kunnen foto's worden gebruikt voor publicaties. Kies hiervoor foto's met de tag GDPR, dan ben je zeker dat de toestemmingen in orde zijn.

Voorbeeld Toestemmingsclausule

Voorbeeld toestemming algemeen

- Ik geef toestemming aan het bestuur om foto's en/of videobeelden op te nemen <tijdens de activiteiten/in het kader van de werking van …> en dat deze beelden kunnen worden gepubliceerd voor zowel interne doeleinden als voor communicatie met het publiek via alle communicatiekanalen van het bestuur zoals de website, het informatieblad, affiches, flyers, het intranet en diverse sociale mediakanalen.

Voorbeeld toestemming gesplitst

- Ik geef toestemming aan het bestuur om foto's en/of videobeelden op te nemen <tijdens de activiteiten/in het kader van de werking van … >
- Deze beelden mogen gepubliceerd worden voor
  - interne doeleinden zoals de communicatie met andere deelnemers, familieleden en personeelsleden;
  - communicatie met het publiek via alle communicatiekanalen van het bestuur zoals de website, het informatieblad, affiches, flyers, en diverse sociale mediakanalen.