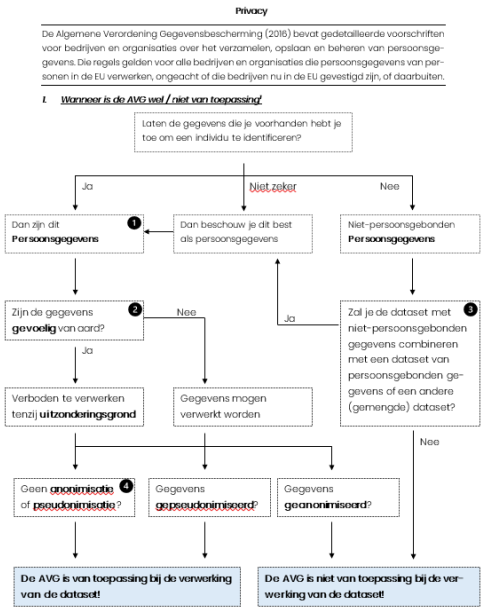
D4A Solution – GDPR Applicability + Roles flow chart

Name of your institution and contact	**Traffic <of> data – BE Pilot** **Vives University of Applied Science – Cedric De Koker**
Place of the implemented solution	South-West-Flanders
Implementation level (e.g. internal, municipal, intercommunal, regional)	Intercommunal (South-West-Flanders)
Dimension	Regulatory
Subdimension	Data governance Data risks
Problem	Local governments possess a large amount of data. However, if they want to make effective use of this data, they will have to navigate a complex and evolving regulatory landscape. Different rules apply to different types of data, e.g. public sector information falls under the Open Data Directive, personal data under de General Data Protection Regulation, raw and pre-processed data generated by connected products under the Data Act, etc. What is possible or required with regard to one (part of a) dataset, might not be with regard to another. It is therefore important for those working within local government to understand what rules apply when and to what data.
Solution	*GDPR Applicability and Roles Flow Chart* helps local officials to determine first whether they are processing personal data and when their actions thus fall within the scope of application of the GDPR. Once it is established that they are processing personal data, the solution helps them determine their exact role under the GDPR (Data controller, Joint data controller, Data processor). Once they know their role, they can pinpoint what legal responsibilities and obligations they have to abide by.
Feedback	Handy solution to help
Format (e.g. Open Source)	PDF
Costs	There is no implementation or operation cost.
Links	The flow chart was distributed during Leiedal's workshops with local municipalities. An English translation will be shared on the D4A-project website.

Screenshots, visuals, images



Privacy

De Algemene Verordening Gegevensbescherming (2016) bevat gedetailleerde voorschriften voor bedrijven en organisaties over het verzamelen, opslaan en beheren van persoonsgegevens. Die regels gelden voor alle bedrijven en organisaties die persoonsgegevens van personen in de EU verwerken, ongeacht of die bedrijven nu in de EU gevestigd zijn, of daarbuiten.

1 ***Wanneer is de AVG wel / niet van toepassing?***

[1] Dit stroomschema en de bijhorende informatie is gebaseerd op de Fiche 'Wanneer is de AVG wel/niet van toepassing?' van het Kenniscentrum Data & Maatschappij.

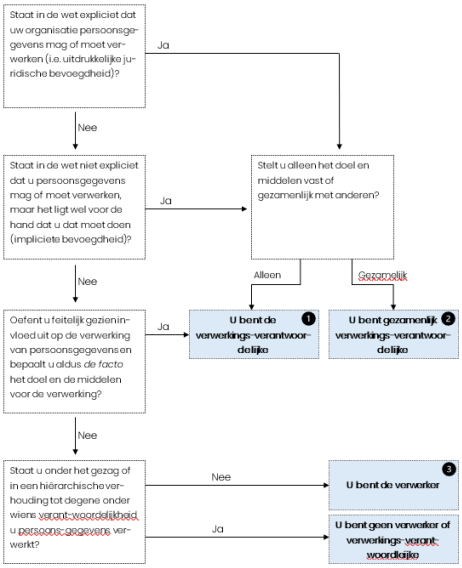
1 **'Persoonsgegevens'** omvatten zowel informatie die toelaat om een persoon te identificeren, als informatie die je aan een persoon kan koppelen. Zodra gegevens toelaten om een levend natuurlijk persoon direct (bv. naam of emailadres) of indirect (door combinatie met andere gegevens, bv. nummerplaat) te identificeren, spreekt men van persoonsgegevens en is de AVG van toepassing. Daarnaast is ook alle informatie die je aan een persoon kan koppelen een persoonsgegeven. Het kan daarbij gaan om digitale of analoge gegevens, ongeacht de vorm (bv. alfabetisch, numeriek of grafisch).

2 Bepaalde persoonsgegevens worden onder de AVG als **'gevoelig'** beschouwd. Deze gegevens mogen in principe niet verwerkt worden tenzij er een uitzonderingsgrond voorhanden is. De lijst van gevoelige gegevens omvat: gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gezondheidsgegevens, gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid en gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

3 Datasets die zowel persoonsgegevens als niet-persoonsgebonden gegevens bevatten, zijn **'gemengde' datasets**. Indien beide soorten van gegevens 'onlosmakelijk met elkaar verbonden zijn' in de gehele dataset, zal de AVG van toepassing zijn op de volledige dataset, ook indien de persoonsgegevens maar een klein deel van de set uitmaken. Indien beide soorten wel afscheidbaar zijn, is de AVG enkel van toepassing op het gedeelte persoonsgegevens, voor zover beide sets ook effectief afgescheiden worden.

4 **Pseudonimisering** verwijst naar het proces waarbij gegevens in een dataset gecodeerd of verborgen worden zodat zij niet meer aan een specifieke natuurlijke persoon kunnen worden gekoppeld zonder aanvullende gegevens die als sleutel dienen. **Anonimisering** verwijst naar het onomkeerbare proces waarbij persoonsgegevens of een dataset die persoonsgegevens bevat zodanig worden bewerkt dat zij niet langer een persoon identificeren of aan een persoon te koppelen zijn. De AVG is niet van toepassing op geanonimiseerde gegevens. Elk risico van her-identificatie moet daartoe worden uitgesloten.

2. *Rollen en verantwoordelijkheden onder de AVG*[2]



[2] Dit stroomschema en de bijhorende informatie is gebaseerd op de Handleiding Algemene Verordening Gegevensbescherming (2019) van de Nederlandse Autoriteit Persoonsgegevens.

1 De **Verwerkingsverantwoordelijke** stelt het doel van en de middelen voor de verwerking van persoonsgegevens vast. Hij dient hierbij

- De gegevens te verwerken in lijn met de AVG-verwerkingsbeginselen.
- Een register van verwerkingsactiviteiten bij te houden (de registerplicht).
- Onder bepaalde omstandigheden een functionaris voor gegevensbescherming aan te stellen.
- Voorafgaand aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffectbeoordeling uit te voeren.
- De Gegevensbeschermingsautoriteit onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit te raadplegen.
- Bij het inrichten van verwerkingen rekening te houden met het principe van *privacy by design & default*.
- Passende beveiligingsmaatregelen te treffen met het oog op de bescherming van persoonsgegevens.
- In het geval van een datalek melding te doen bij de Gegevensbeschermingsautoriteit en desgevallend ook bij de betrokkenen.
- Afspraken te maken met verwerkers.
- Medewerking te verlenen aan de Gegevensbeschermingsautoriteit.

2 In het geval van **gezamenlijk verwerkingsverantwoordelijkheid** zijn alle organisaties verantwoordelijk voor de gezamenlijke verwerking. Elke deelnemende organisatie kan door betrokkenen worden aangesproken.

3 De **verwerker** verwerkt persoonsgegevens in opdracht van een andere organisatie. De verwerker gebruikt deze persoonsgegevens niet voor eigen doeleinden en voert de verwerkingen alleen feitelijk uit. De belangrijkste verplichtingen van een verwerker zijn:

- De verwerker mag alleen handelen in opdracht van de verwerkingsverantwoordelijke.
- De verwerker wordt verplicht een overzicht bij te houden van alle categorieën persoonsgegevens die hij verwerkt in opdracht van de verwerkingsverantwoordelijke (registerplicht).
- De verwerker moet passende technische en organisatorische beveiligingsmaatregelen nemen die een passend beschermingsniveau bieden met het oog op het risico van de gegevensverwerking voor betrokkenen.
- De verwerker mag geen subverwerkers inschakelen zonder toestemming van de verwerkingsverantwoordelijke.
- De verwerker moet de verwerkingsverantwoordelijke onverwijld op de hoogte stellen van een datalek.
- De verwerker is verplicht medewerking te verlenen bij een verzoek van de toezichthouder in het kader van de uitoefening van diens taken.
- De verwerker dient in bepaalde gevallen een functionaris voor gegevensbescherming aan te stellen.