## Bijlage Toelichting aanleveren documentatie met privacygevoelige gegevens

Het proces van het aanvragen en verstrekken van EFRO-subsidie in het kader van het Operationeel Programma Kansen voor West II verloopt volledig digitaal. Alle uitwisseling van informatie tussen de penvoerder en de Managementautoriteit vindt plaats via het webportaal van Kansen voor West.

Dit betekent dat voortgangsrapportages en bewijsmateriaal voor de rechtmatigheid van de opgevoerde kosten digitaal bij de Managementautoriteit moeten worden aangeleverd. Indien in de projectbegroting loonkosten van medewerkers van organisatie(s) worden opgevoerd, welke in het project als begunstigde zijn opgenomen, moeten ter onderbouwing van deze kosten loonstaten of jaaropgaven van de voor het project werkzame medewerkers bij de managementautoriteit worden ingediend. Ook dit laatste dient digitaal te gebeuren. Houdt er rekening mee dat wij, in verband met de nieuwe privacy wetgeving, loonstaten en/of jaaropgaven willen ontvangen zonder Burgerservicenummers. Indien Burgerservicenummers op de loonstaten en/of jaaropgaven staan, deze gelieve zwart te maken alvorens deze te uploaden.

In de praktijk worden vragen gesteld over de rechtsgeldigheid van deze voorwaarde in het kader van de van toepassing zijnde privacywetgeving, meer specifiek de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG.

Deze toelichting gaat in op de wettelijke verplichtingen waaraan de uitwisseling van informatie en de verwerking van gegevens in het kader van de uitvoering van het EFRO-programma moet worden voldaan. Binnen deze context kan op de volgende wijzen voldaan worden aan de wetgeving op het gebied van de bescherming van persoonsgegevens. Deze wettelijke verplichtingen vormen ook de rechtsgrond voor verwerking van persoonsgegevens onder de AVG, artikel 6 lid 1 sub c.

Wettelijk kader

Het gebruik van een elektronisch systeem voor de uitwisseling van informatie tussen begunstigden en de Managementautoriteit is verplicht op grond van de Europese regelgeving.

Deze verplichting, alsmede de nadere voorwaarden waaraan de systemen moeten voldoen, zijn in de Europese verordeningen op de volgende plaatsen terug te vinden:

* Artikel 122 lid 3 van verordening 1303/2013, één van de belangrijkste verordeningen voor de uitvoering van het EFRO-programma, schrijft voor dat de uitwisseling van alle informatie tussen begunstigden en de managementautoriteit door middel van elektronische systemen voor gegevensuitwisseling plaatsvindt.
* Artikel 125 lid 2 onder d van diezelfde verordening schrijft voor dat de managementautoriteit een gecomputeriseerd systeem opzet voor de vastlegging en opslag van gegevens.
* In uitvoeringsverordening 1011/2014 zijn nadere voorwaarden voor de systemen voor elektronische gegevensuitwisseling opgenomen. De systemen voor elektronische gegevensuitwisseling dienen de beveiliging, de integriteit en de vertrouwelijkheid van de gegevens en de authenticatie van de verzender te waarborgen (artikel 9). Bij de verwerking van informatie dient de bescherming van de persoonsgegevens van natuurlijke personen gewaarborgd te worden (artikel 10).
* In uitvoeringsverordening 821/2014 zijn nadere voorwaarden voor de systemen voor vastlegging en opslag van gegevens opgenomen. Het systeem voor vastlegging en opslag van gegevens moet interoperabel zijn met het systeem voor elektronische gegevensuitwisseling (artikel 8). De elektronische opslagfaciliteit dient beschermd te zijn tegen elk gevaar van verlies of wijziging van de integriteit (artikel 7). De beveiliging van de informatie-uitwisseling en de bescherming van persoonsgegevens dienen te voldoen aan internationale normen en nationale wettelijke voorschriften (artikel 11).
* In de algemene verordening gegevensbescherming (2016/679) worden regels gesteld voor de bescherming van persoonsgegevens bij de verwerking van informatie.
* Tevens is in het Financieel Regelement (Vo.966/2012) toegelicht in art. 59 lid 4 onder verwijzing naar Vo.95/46 dat wij zorgvuldig en binnen de grenzen van de privacy regelgeving met de gegevens om dienen te gaan qua opslag, beveiliging e.d.

Op 25 mei 2018 zijn de Algemene Verordening Gegevensbescherming (2016/679) en de Uitvoeringswet AVG in werking getreden waarin belangrijke bepalingen zijn opgenomen voor het rechtmatig omgaan met persoonsgegevens die door middel van een geautomatiseerd systeem worden verwerkt. Samenvattend komen deze bepalingen er op neer dat persoonsgegevens alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier mogen worden verwerkt, dat persoonsgegevens alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld en verwerkt, dat de gegevensverwerking op een passende manier moet worden beveiligd, dat gegevens slechts zo lang worden gearchiveerd als wettelijk noodzakelijk en last but not least dat degene van wie de persoonsgegevens worden verwerkt (de betrokkene) hiervoor ondubbelzinnig toestemming moet hebben gegeven en moet begrijpen voor welk doel hij de toestemming geeft en welke rechten hij heeft als betrokkene.

Borging kwaliteitsniveau systemen

Uit bovenstaande volgt dat de systemen voor gegevensuitwisseling en voor de vastlegging en opslag van gegevens moeten worden beschermd door adequate beveiligingsmaatregelen en moeten voldoen aan technische eisen zoals vervat in internationale en nationale normen en wettelijke voorschriften.

In het kader van het beheers- en controlesysteem van het EFRO-programma wordt door middel van assessments en audits de opzet en werking van bedoelde systemen periodiek getoetst. Daarbij dienen internationale standaarden qua beveiliging en gegevensbescherming te worden geborgd. Jaarlijks wordt een en ander gecontroleerd door de Auditdienst Rijk.

Persoonsgegevens

In het kader van een juiste duiding van begrippen is van belang wat in de wettelijke context precies onder persoonsgegevens wordt verstaan. Alle gegevens die informatie bevatten over een identificeerbare natuurlijke persoon zijn persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming. Is de betrokkene niet identificeerbaar, dan is het gegeven geen persoonsgegeven. Een persoon is identificeerbaar als de identiteit van de persoon redelijkerwijs zonder onevenredige inspanning kan worden vastgesteld. Gegevens die van bijvoorbeeld naam, adres en woonplaats zijn ontdaan, zijn veelal niet direct identificerend. Echter bijvoorbeeld in combinatie met andere gegevens kunnen dergelijke gegevens toch weer tot een bepaalde persoon leiden, waardoor de persoon indirect identificeerbaar is. Het al dan niet (indirect) identificeerbaar zijn van natuurlijke personen hangt nauw samen met de feitelijke omstandigheden en de feitelijke mogelijkheden die de verantwoordelijke voor de gegevensverwerking (de managementautoriteit) heeft.

Naleven van wet- en regelgeving bij het aanleveren van privacygevoelige informatie door begunstigden

Uit het bovenstaande volgt dat de Managementautoriteit verplicht is voor de uitvoering van het EFRO-programma een digitaal systeem voor de uitwisseling en opslag van gegevens te gebruiken. Dit systeem dient in het kader van de van toepassing zijnde regelgeving op het gebied van privacy te voldoen aan strenge technische eisen op het gebied van de bescherming van persoonsgegevens.

Gegevens zoals loonstaten en jaaropgaven zijn te beschouwen als persoonsgegevens als deze documenten informatie bevatten over identificeerbare natuurlijke personen of als de identiteit van die persoon zonder onevenredige inspanning door de managementautoriteit kan worden vastgesteld.

Medewerkers uit de organisatie(s) (begunstigden binnen het project), waarvan loonkosten worden opgevoerd in de projectbegroting, om toestemming te vragen om loonstaten of jaaropgaven ter onderbouwing van projectkosten aan de managementautoriteit te verstrekken. Het document waarin de medewerker deze toestemming geeft dient onderdeel uit te maken van de projectadministratie.

Een (andere) mogelijkheid is dat loongegevens worden geanonimiseerd. Hiervoor geldt als voorwaarde dat de authenticiteit van het document nog wel vastgesteld moet kunnen worden en er door de managementautoriteit een relatie te leggen moet zijn tussen de inschaling en de in het project opgevoerde loonkosten. Bij deze keuze voor verstrekking van de loongegevens is het van de feitelijke omstandigheden afhankelijk of de identiteit van de natuurlijke persoon (indirect) door de managementautoriteit vastgesteld kan worden. Het kan met andere woorden nog steeds noodzakelijk zijn dat de betreffende natuurlijke personen om toestemming moet worden gevraagd om de gegevens te verstrekken.

In aanvulling hierop is het voor partners binnen samenwerkingsprojecten mogelijk de bedoelde documenten niet via de penvoerder aan de managementautoriteit te verstrekken. Ook dan blijven de regels voor het vragen van toestemming aan de natuurlijk persoon in geval van verstrekking van persoonsgegevens van kracht, maar er is geen derde partij (de penvoerder) mede verantwoordelijk. Aan de contactpersoon bij Kansen voor West kan worden aangegeven dat van deze mogelijkheid gebruik zal worden gemaakt.

Helaas is het onmogelijk om ter plekke alle persoonsgevoelige gegevens in te komen zien, bovendien moeten de brondocumenten voor de ons controlerende instanties beschikbaar zijn in ons systeem ter voorkoming van dubbel opvragen.