Inhoud: Kaarten met motto en uitleg hoe DUTO een bijdrage kan leveren aan het **beschermen van persoonsgegevens (AVG)** op basis van gedeelde belangen

Te gebruiken door: Informatieprofessionals

Te gebruiken voor: Voorbereiden van gesprekken of presentaties met c.q. voor **privacy-officers**. Met als doel win-win situaties te creëren en samen te werken.
De kaarten geven hiertoe 'ingrediënten' of inspiratie (niet bedoeld om als zelfstandig te lezen document te geven).

Aandacht trekken	**By design: samen vooraf bouwen aan gedeelde belangen**
Interesse opwekken	Jouw organisatie heeft een nieuwe applicatie voor personeelsbeheer aangeschaft. Je bent als privacy officer hier te laat bij betrokken. Dit heeft tot gevolg dat bij inrichten van de applicatie de functionaliteit rondom het vernietigen van persoonsgegevens niet is meegenomen. En achteraf herstellen kost geld en tijd. Hoe kun je dit in de toekomst voorkomen? Door by design te werken “By design" betekent dat een eigenschap, zoals privacy of duurzame toegankelijkheid, vanaf het begin in het ontwerp van een product, systeem of proces is ingebouwd. Het is geen achteraf toegevoegde optie, maar een fundamenteel onderdeel van de ontwikkeling om risico's te minimaliseren en aan vereisten (zoals de AVG) te voldoen. Zo werk je proactief en preventief en zijn vereisten ingebouwd in het systeem of proces.
Gedeeld belang benadrukken	Door samen op te trekken bij het inrichten van informatiesystemen kunnen we de belangen vanuit privacy én informatiebeheer borgen. • Als privacy officer ga je uit van **privacy by design** en **by default**: je houdt rekening met de bescherming van persoonsgegevens bij de inrichting van informatiesystemen. Deze bescherming moet de *regel* zijn en *niet de uitzondering*. • Als informatiebeheerder ga je uit van **archiveren by design:** Je houdt rekening met informatiebeheer bij de inrichting van informatiesystemen. We willen voorkomen dat achteraf blijkt dat er geen rekening is gehouden met privacy of DUTO: bepaalde technische voorzieningen of functionaliteiten zijn er niet. Of kunnen pas achteraf met veel moeite en hoge kosten gerealiseerd worden.
Activeren	Ga samen aan de slag: • Maak afspraken over by design aanpak; een gezamenlijke werkwijze bij inrichting van informatiesystemen. **Tip:** gebruik de handreiking Archiveren by design

Aandacht trekken	**Een gezamenlijke risicobeoordeling leidt tot passender maatregelen**
Interesse opwekken	Jouw organisatie krijgt een nieuwe taak waarbij veel persoonsgegevens verwerkt zullen worden. Je wilt een DPIA (*data protection impact assessment*) uitvoeren. Zodat privacyrisico's in beeld worden gebracht. En om maatregelen te nemen die die risico's verminderen. De proceseigenaar stribbelt wat tegen omdat er ook al een DUTO-risicobeoordeling is uitgevoerd
Gedeeld belang benadrukken	Ook informatieprofessionals voeren een risicobeoordeling uit. Het doel is om risico's in beeld te brengen als informatie niet duurzaam toegankelijk is*). En om passende maatregelen te nemen die risico's verminderen en duurzame toegankelijkheid van overheidsgegevens bevorderen. De bevindingen uit een **DUTO-risicobeoordeling** en een **DPIA** kunnen elkaar versterken. Ze kunnen leiden tot aanbevelingen om informatiesystemen aan te passen aan de hand van het DUTO-raamwerk. En zo risico's verkleinen die bestaan op het gebied van duurzame toegankelijkheid met implicaties voor bescherming van persoonsgegevens. *) Het voorstel voor de nieuwe Archiefwet eist namelijk dat organisaties passende maatregelen nemen voor duurzame toegankelijkheid van overheidsinformatie.
Activeren	Ga samen aan de slag: • Werk samen aan DPIA's en DUTO-risicobeoordelingen. Zie ook de Handreiking DUTO-risicobeoordeling

Aandacht trekken	**Overzicht geeft rust**
Interesse opwekken	Jouw organisatie wil het beheer van persoonsgegevens van bepaalde werkprocessen door een externe leverancier laten uitvoeren. Om een verwerkersovereenkomst te maken, heb je inzicht nodig om welke persoonsgegevens dit gaat. Echter je hebt geen overzicht waar te beginnen. Een must-have] voor het beschermen van persoonsgegevens en en DUTO is een actueel overzicht van de overheidsinformatie (inclusief persoonsgegevens) die je als overheidsorganisatie verwerkt en beheert. Heb je dit niet of deze is niet actueel, dan neemt het risico toe dat er geen inzicht is of en hoe persoonsgegevens op meerdere plekken binnen de organisatie verwerkt worden. En dat een zoekopdracht niet alle verwerkingen in kaart brengt. Heb je daarentegen een actueel overzicht van de overheidsinformatie die jouw organisatie verwerkt en beheert, dan kun je erop vertrouwen dat dit de daadwerkelijke situatie weergeeft zoals deze is. Dat geeft rust.

Gedeeld belang benadrukken	Een actueel overzicht draagt verder bij aan:
	
	• Gericht en effectief een **DPIA** uitvoeren.
	Overzicht biedt inzicht in:
	  • De wettelijke grondslag voor het verwerken van persoonsgegevens
	  • Waar persoonsgegevens worden opgeslagen en beheerd
	  • Wie toegang heef tot die gegevens
	  • Met welke andere organisaties persoonsgegevens gedeeld worden in het kader van bijvoorbeeld samenwerkingsverbanden
	• Een verwerkingsregister opstellen en actualiseren.
	• De verzoeken van burgers rondom bescherming van hun persoonsgegevens efficiënter behandelen.
	Zo kan de burger een verzoek om inzage doen. Daarmee kan de burger controleren of de persoonsgegevens die organisaties van hen verwerken, kloppen. Zonder overzicht is de kans groot dat er essentiële (samenhangende) informatie over het hoofd wordt gezien. En dat het verzoek meer tijd gaat kosten
	• Dataminimalisatie bevorderen.
	Dataminimalisatie is een basisprincipe uit de AVG. Om dat principe in de praktijk te brengen, is het noodzakelijk om een goed overzicht te hebben. Zodat je overbodige verwerking en opslag van persoonsgegevens kunt vermijden.

Activeren	Ga samen aan de slag:
	
	• Bepaal samen of de huidige overzichten van overheidsinformatie (inclusief persoonsgegevens) voldoende inzicht bieden om aan jullie behoeften en die van de organisatie te kunnen voldoen.
	Tip: Gebruik de handreiking DUTO-risicobeoordeling.
	• Neem passende maatregelen als de overzichten er niet zijn of niet voldoen.
	Denk daarbij aan DUTO modeleisen, zoals:
	  • inrichten van een zoekfunctionaliteit (o.a. modeleis B13).
	  • op (selecties van) de informatieobjecten en de bijbehorende metagegevens kunnen zoeken (T10). Hierdoor kan een verzoek tot inzage efficiënter en rechtmatig afgehandeld worden.

Aandacht trekken	**Regie op persoonsgegevens met metagegevens**
Interesse opwekken	Jouw organisatie ontvangt een verzoek van een burger waarbij deze inzage in persoonsgegevens vraagt. Dit is een zeer belangrijke doch tijdrovende klus. Met metagegevens kun je persoonsgegevens en de vewerkingen hiervan sneller in samenhang en in verschillende contexten vinden. Met metagegevens heb je meer regie op persoonsgegevens. Als medewerkers of systemen bij creatie van persoonsgegevens niet de juiste metagegevens aanbrengen, dan kan bescherming van persoonsgegevens gevaar lopen. Het is dan namelijk onduidelijk op welke grondslag, voor welke specifieke doelen en voor hoelang persoonsgegevens verwerkt mogen worden
Gedeeld belang benadrukken	Metagegevens geven betekenis en context aan persoonsgegevens. Ze geven antwoord op de vragen wie, wat, waar, waarom, wanneer en hoe. Met deze informatie kun je sneller en makkelijker persoonsgegevens vinden en bovendien weet je [met welk doel persoonsgegevens binnen de desbetreffende context worden verwerkt (doelbinding). Ook dragen metagegevens bij aan dat je kunt aantonen dat er rechtmatig met persoonsgegevens omgegaan wordt.
Activeren	Ga samen aan de slag: • Onderzoek samen hoe metagegevens binnen de organisatie worden gebruikt en beheerd. Is hiervoor een metagegevensschema? Het hebben van een metagegevensschema is een randvoorwaarde in het DUTO-raamwerk. Om deze randvoorwaarde in te vullen heeft het Nationaal Archief de norm Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie (MDTO) ontwikkeld (RVW12). • Neem zonodig passende maatregelen om de functie metagegevensbeheer in te vullen. Het DUTO-raamwerk bevat modeleisen voor het inrichten van de functie metagegevensbeheer (F06).

Aandacht trekken	**Wat er niet is, kan ook niet gelekt worden**
Interesse opwekken	Jouw organisatie heeft te maken met een datalek van persoonsgegevens. Uit onderzoek blijkt dat het hier om persoonsgegevens gaat die allang vernietigd hadden moeten zijn. Een vastgestelde vernietigingsprocedure en een ingerichte functionaliteit voor vernietigen, verkleinen het risico dat persoonsgegevens onrechtmatig worden verwerkt nà het verlopen van de wettelijke bewaartermijn uit de selectielijst. Wat er niet is, hoeft niet beschermd te worden en kan ook niet gelekt worden. Vernietigen verbindt de AVG en de Archiefwet. Het in samenhang vormgeven van processen, procedures en functionaliteiten op het gebied van vernietigen is nodig.
Gedeeld belang benadrukken	Tijdig vernietigen draagt verder bij aan: • Risico op datalekken verkleinen. • Voldoen aan AVG-beginselen als **dataminimalisatie** en **opslagbeperking**. Deze eisen o.a. van overheidsorganisaties dat ze informatie tijdig vernietigen. • Voldoen aan **recht op vergetelheid**. Burgers kunnen een verzoek bij een organisatie indienen om hun persoonsgegevens te vernietigen. De organisatie houdt hierbij rekening met bewaartermijnen uit de selectielijst. • Voldoen aan **doelbinding**. Zo moet een organisatie persoonsgegevens die ongevraagd toegezonden zijn en niet nodig zijn voor het desbetreffende werkproces, [CW1] op rechtmatige wijze vernietigen of terugsturen naar de betrokkene.
Activeren	Ga samen aan de slag: • Onderzoek samen hoe vernietigen binnen de organisatie plaatsvindt. **Tip:** Gebruik hierbij de handreiking DUTO-risicobeoordeling. • Neem zonodig passende maatregelen op het gebied van vernietigen. **Tip:** Vernietigen is een van de vijf DUTO-processen in het DUTO-raamwerk. In de module over dit DUTO-proces vind je welke zaken binnen informatiesystemen ingericht moeten worden om rechtmatig en gecontroleerd te vernietigen. Inclusief modeleisen op dit gebied. • **Tip:** Om digitaal te kunnen vernietigen, gebruik je de Handreiking Digitaal vernietigen

Aandacht trekken	**Organiseer toegang. Bescherm persoonsgegevens.**
Interesse opwekken	Jouw organisatie heeft het nieuws gehaald omdat onbevoegde medewerkers toegang hadden tot bijzondere persoonsgegevens van een bekende Nederlander. Alleen bevoegde gebruikers mogen persoonsgegevens inzien of verwerken. Als je het toegangsbeheer goed organiseert en inricht , dan verklein je het risico op ongeoorloofde toegang tot (bijzondere categorieën) persoonsgegevens.
Gedeeld belang benadrukken	Toegang organiseren draagt verder bij aan: • Doelbinding garanderen. Doelbinding vereist ook dat oneigenlijke toegang verhinderd of ontmoedigd wordt. Dat kan aan de hand van toegangsbeheer en logging Met logging kun je achteraf controleren of gebruikers geautoriseerd overheidsinformatie (of persoonsgegevens) ingezien hebben. • Overheidsinformatie op passende manier openbaar maken. Soms moet overheidsinformatie openbaar gemaakt kunnen worden, bijvoorbeeld in het kader van een verzoek op grond van de Wet open overheid. Als zich in die overheidsinformatie bijzondere categorieën persoonsgegevens bevinden, dan wordt deze in principe uitgezonderd van openbaarmaking (art.5.1, lid 1d Woo). Gegevens kunnen dan worden gelakt. • Krachten bundelen met andere informatiespecialisten. Toegangsbeheer is een belangrijke randvoorwaarde voor duurzame toegankelijkheid van overheidsinformatie.
Activeren	Ga samen aan de slag: • Zoek de samenwerking op met specialisten op het gebied van informatiebeveiliging, privacy en informatiebeheer om toegang te organiseren. Doorlopend actueel beheer van toegangsrechten voor gebruikers (zie ook de toelichting op dit thema in de BIO) en het inrichten van Identity and Access Management zijn randvoorwaarden voor duurzame toegankelijkheid (RVW06 en RVW07). • Onderzoek gezamenlijk hoe toegang is georganiseerd in de organisatie. Neem zonodig passende maatregelen om dit te verbeteren. Gebruik hiertoe modeleisen uit het DUTO-raamwerk: • F11: het inrichten van functionaliteit rondom toegangsbeheer • F05; T12-13: maskering (zoals lakken)