AVG GAP Analyse

En verwerkingsregistratie

Classificatie	Vertrouwelijk
Gegenereerd door	www.classity.nl

Verwerkingsregistratie Webshop order

Algemeen	
Betrokken informatiesystemen	Magento Webshop
Business verantwoordelijke	Jeroen de Wit
IT verantwoordelijke	Mirella de Visser
Er worden gegevens betrokken van	FlowerPower (DropShip)
Er worden gegevens geleverd aan	PickAndSend (FullFill)
Er worden gegevens naar derden landen geexporteerd	Nee

Details van de verwerking	
De volgende typen persoonsgegevens worden verwerkt	Klanten. Klein zakelijke contacten.
De volgende categorieen persoonsgegevens worden verwerkt	NAW. Telefoon- en faxnummers. E-mailadressen. Vorderingen. Facturen. Orders. Accountgegevens (wachtwoorden).
Bijzondere persoonsgegevens	
Verwerkingsdoelen	- Bestelling registreren - Order picken en labellen - Pakket aanmelden bij verzender - Facturatie - Orderstatus versturen - Tevredenheidsonderzoek uitvoeren - After sales service verlenen
Registratie uitdrukkelijke toestemming	
Bekende bewaartermijnen	NAW (12). Telefoon- en faxnummers (12). E-mailadressen (12). Vorderingen (96). Facturen (96). Orders (96). Accountgegevens (wachtwoorden) (99999).
Verwerkingsgrondslag	Overeenkomst.
Getroffen beveiligingsmaatregelen	Er is een formeel vastgesteld informatiebeveiligingsbeleid aanwezig dat ook is geimplementeerd. Er is logische toegangsbeveiliging geimplementeerd. Er zijn maatregelen voor fysieke toegangsbeveiliging. Er wordt gebruik gemaakt van een kluis. Alle beveiligingsverantwoordelijkheden zijn, zowel op sturend als op uitvoerend niveau, duidelijk gedefinieerd en belegd. In zelf gebouwde applicaties ingebouwde beveiligingsmaatregelen. Er is een continuiteitsplan waarmee de kans dat persoonsgegevens door calamiteiten onherstelbaar verloren kunnen gaan tot een acceptabel niveau worden gereduceerd. Er is periodieke controle op de naleving van de maatregelen.
Optionele toelichting	

Resultaten GAP Analyse

In de onderstaande tabellen is per onderwerp aangegeven welke activiteiten er resteren om voor deze verwerking (Webshop order) invulling te geven aan de relevante aandachtspunten uit de AVG.

Verwerkingsgrondslag

Doelstelling	Status
De wettelijke grondslag voor de verwerking is vastgesteld en vastgelegd (bijv.: vanuit overeenkomst, toestemming, gerechtvaardigd belang).	Voldoet
Persoonsgegevens worden alleen verwerkt voor het doel waarvoor ze primair zijn afgestaan, tenzij er voor specifieke andere doelen ondubbelzinnige toestemming is verkregen en vastgelegd. Hierbij zijn klanten goed geinformeerd over waarvoor zij exact toestemming verlenen.	Voldoet

Documenteren

Doelstelling	Status
Deze verwerking van persoonsgegevens is vastgelegd in het verwerkingsregister.	Voldoet
Bij het vragen van toestemming voor een specifieke verwerking wordt geregistreerd: - Waar toestemming voor is gegeven; - Waar en wanneer de toestemming is gevraagd; - Hoe wij de toestemmingsvraag hebben gesteld (en waarover wij hebben geinformeerd).	Voldoet
Voor de verwerking van bijzondere categorieen van persoonsgegevens (medisch/etniciteit/geloofsovertuiging/etc.) is altijd een ondubbelzinnige toestemming gevraagd en vastgelegd.	Voldoet
Er ligt vast voor welke gegevens een specifieke wettelijke bewaarplicht geldt. Deze bewaarplicht wordt bij een verzoek tot gegevenswissing niet uit het oog verloren.	Voldoet
Van gegevens van kinderen (tot 16 jaar) is de toestemming van de ouder of voogd vastgelegd.	Voldoet
Met alle partijen waarmee wordt samengewerkt is (in samenspraak met de juristen) een verwerkersovereenkomst afgesloten. Benodigde actie: Verwerkersovereenkomst afsluiten met fullfillment partner. Benodigde resources: Privacy Officer, ICT Architect	Voldoet niet

Rechten betrokkenen

Doelstelling	Status
De gegevens die over een persoon verzameld zijn kunnen op verzoek binnen 3 weken worden gewist.	Voldoet
Op verzoek kan binnen 3 weken een kopie van de over iemand verwerkte persoonsgegevens worden aangeleverd, inclusief de doelen waarvoor de gegevens verzameld zijn.	Voldoet
Aan betrokkenen te leveren kopieen van verwerkte persoonsgegevens zijn in een uniform, voor machines leesbaar formaat, beschikbaar.	Voldoet
Gegevensverwerkingen kunnen voor specifieke personen (binnen 3 weken) worden opgeschort op het moment dat daar recht op is (blokkeren mutaties, bevriezen van de gegevens). Benodigde actie: Mogelijkheid tot opschorting van verwerken persoonsgegevens onderzoeken en implementeren. Benodigde resources: ICT Architect, Senior ontwikkelaar, Technisch Specialist	Voldoet niet
Doorgegeven actualisaties of correcties van persoonsgegevens kunnen binnen 3 weken worden doorgevoerd.	Voldoet
Verzoeken tot correctie/actualisatie/ verwijdering/opschorting van (het gebruik van) persoonsgegevens kunnen overal worden doorgevoerd, ook als verwerkingen aan andere afdelingen, organisatieonderdelen of derden zijn uitbesteed. Hierbij wordt rekening gehouden met verplichtingen uit andere / meer zwaarwegende regelgeving. Denk aan langere bewaarverplichting a.g.v. belastingwetgeving voor specifieke financiele gegevens. Benodigde actie: Afspraken maken met drop shipment partner, implementeren in drop shipment koppeling Benodigde resources: ICT Architect, Senior ontwikkelaar, Technisch Specialist	Voldoet niet
Binnen systemen en processen waarin geprofileerd is het mogelijk om specifieke personen (die dit aangeven) van deze geautomatiseerde verwerking uit te sluiten. We spreken van profilering indien beslissingen enkel op een geautomatiseerde verwerking zijn gebaseerd (data analytics, big data).	Voldoet
Er is gefaciliteerd dat een verstrekte toestemming voor het verwerken van persoonsgegevens door een persoon net zo makkelijk kan worden ingetrokken als dat hij is afgegeven.	Voldoet

Privacy by design & by default

Doelstelling	Status
Voordat persoonsgegevens worden verstrekt (geldt ook voor: corrigeren/actualiseren/ verwijderen/blokkeren) wordt altijd de identiteit van de persoon die dit verzoekt vastgesteld. Hierbij wordt rekening gehouden met eventuele uitzonderingen en vastgelegde machtigingen.	Voldoet
Persoonsgegevens verwerkende systemen en processen zijn privacy-vriendelijk ontworpen en standaard staan verwerkingsinstellingen (waaronder toestemmingen) zo privacy-vriendelijk mogelijk ingesteld. (privacy by design, privacy by default).	Voldoet
De verwerkte persoonsgegevens zijn geclassificeerd. Hierbij vindt classificatie plaats op beschikbaarheid, integriteit en vertrouwelijkheid.	Voldoet
Bij hogere classificatie-uitkomsten is een risicoanalyse/PIA uitgevoerd om aanvullende maatregelen te bepalen. Deze maatregelen zijn geimplementeerd.	Voldoet
Er is een PIA uitgevoerd indien de verwerkingsactiviteiten een hoog risico voor de betrokkenen met zich mee kan brengen.	Voldoet
Gegevens worden niet langer dan noodzakelijk is bewaard.	Voldoet
Indien het voor een specifieke verwerking niet noodzakelijk is dat gegevens tot op de persoon herleidbaar zijn, zijn anonimisatie- en pseudonimisatietechnieken toegepast.	Voldoet
Gegevens die worden ingezet om de dienstverlening te optimaliseren, te testen en om producten te verbeteren, worden daarvoor geanonimiseerd of gepseudonimiseerd.	Voldoet
Alle maatregelen die volgen uit het beveiligingsbeleid (en de daarvan afgeleide baseline) zijn toegepast.	Voldoet

Organisatie

Doelstelling	Status
Er is een privacy officer aangesteld met voldoende kennis en steun en mandaat van het bestuur om de verantwoordelijkheid voor het borgen van een passende bescherming van persoonsgegevens op zich te nemen.	Voldoet
Het privacybeleid houdt rekening met de uitgangspunten uit de AVG en beschrijft hoe de privacyrollen en verantwoordelijkheden in de organisatie zijn belegd.	Voldoet
Het beveiligingsbeleid houdt rekening met de uitgangspunten uit de AVG en beschrijft hoe de beveiligingsrollen en verantwoordelijkheden in de organisatie zijn belegd. Benodigde actie: Beveiligingsbeleid actualiseren Benodigde resources: Security Officer	Voldoet niet
Er is vastgelegd op welke wijze een datalek goed kan worden afgehandeld.	Voldoet
Er is vastgelegd op welke wijze er invulling wordt gegeven aan werkzaamheden die gerelateerd zijn aan betrokkenen die gebruik maken van hun rechten (inzien/verwijderen/muteren/bevriezen/bezwaar tegen profilering).	Voldoet