Bezoekadres De Wel 14-16 3871 MV Hoevelaken
Postadres Postbus 44 3870 CA Hoevelaken
Telefoon 033 - 258 04 60
E-mail secretariaat@contactgroepautomatisering.nl
Web www.contactgroepautomatisering.nl

Contactgroep Automatisering

Whitepaper Privacy

Waarom deze whitepaper?

De Stichting Contactgroep Automatisering acht het belangrijk en noodzakelijk dat het voor gebruikers van automatiseringssystemen duidelijk is aan welke verplichtingen zij dienen te voldoen met betrekking tot het borgen van de privacy van haar klanten. Door middel van de deze whitepaper wil de stichting bijdragen aan het scheppen van duidelijkheid over de wet- en regelgeving met betrekking tot privacy. In de whitepaper worden de belangrijkste privacyaspecten behandeld met betrekking tot de samenwerking tussen een automatiseringsbedrijf en een financieel dienstverlener die gebruik maakt van de systemen van dat bedrijf.

Wie is de Stichting Contactgroep Automatisering (SCA)?

De Stichting Contactgroep Automatisering is een stichting die is opgericht om de bewustwording bij financieel adviseurs te vergroten van de gevolgen die de digitalisering van de financiële sector voor de bedrijfsvoering van deze adviseurs gaat hebben. Daarnaast fungeert de SCA als een centraal platform voor partijen die in overleg willen treden met leveranciers van software die wordt gebruikt door financieel adviseurs. Hieronder vallen partijen zoals de AFM, Adfiz, HDN, et cetera.

Wat beoogt de Wet bescherming persoonsgegevens?

De Wet bescherming persoonsgegevens (Wbp) is een wet die vereisten stelt aan de omgang met persoonsgegevens van burgers. De wet is voor het grootste gedeelte gebaseerd op Europese wet- en regelgeving. In de wet wordt bepaald wat onder persoonsgegevens moet worden verstaan en welke partij de verantwoordelijkheid draagt voor de zorgvuldige omgang met de persoonsgegevens, ook als de gegevens naar een derde worden verstuurd.

Wat zijn persoonsgegevens en wanneer verwerk ik die?

Persoonsgegevens zijn gegevens die zien op natuurlijke personen. Dat betekent dat gegevens over een bedrijf (een rechtspersoon), niet worden gezien als een persoonsgegeven. Dit kan alleen anders zijn indien de naam verwijst naar een natuurlijk persoon. De hoofdregel is dat wanneer door middel van bepaalde gegevens een natuurlijk persoon kan worden geïdentificeerd, er sprake is van persoonsgegevens.

Voorbeelden van persoonsgegevens: NAW-gegevens, e-mailadressen, gegevens over financiële omstandigheden en gegevens over iemands gezondheid. Door de Wbp wordt er onderscheid gemaakt tussen algemene en bijzondere persoonsgegevens.

Algemene persoonsgegevens zijn alle persoonsgegevens die geen bijzondere persoonsgegevens zijn. Bijzondere persoonsgegevens zijn gegevens betreffende:

- godsdienst of levensovertuiging;
- ras;
- politieke voorkeur;
- gezondheid*;
- seksuele leven;
- lidmaatschap van een vakbond;
- strafrechtelijk verleden*;
- Burgerservicenummer (BSN)*.

De met * gemarkeerde gegevens, komen in veel administraties van financieel advieskantoren voor.

Een bedrijf verwerkt persoonsgegevens indien het een handeling verricht met persoonsgegevens. In de praktijk verwerkt men nagenoeg altijd persoonsgegevens indien men persoonsgegevens ontvangt en/of verzamelt van klanten. De reikwijdte van de definitie van verwerken loopt van het verzamelen zelf tot het vernietigen van de persoonsgegevens. De hoofdregel is dat een bedrijf enkel persoonsgegevens mag verwerken indien zij daar een wettelijke grond voor heeft. Bijvoorbeeld omdat zij toestemming heeft verkregen van de persoon op wie de gegevens zien, of omdat zij de persoonsgegevens verwerkt om een overeenkomst uit te voeren die is gesloten tussen de persoon en het bedrijf.

Wat is een bewerkersovereenkomst?
Als een financieel dienstverlener ervoor kiest om gebruik te maken van automatiseringssoftware waarin persoonsgegevens worden verwerkt, zal er in sommige gevallen met de leverancier van de software een overeenkomst moeten worden gesloten om te borgen dat er veilig met de persoonsgegevens wordt omgegaan. De hoofdregel is: worden er tijdelijk of langdurig persoonsgegevens gestald bij een softwareleverancier die de gegevens in opdracht van de financieel dienstverlener bewerkt (opslaat, gebruikt voor berekeningen, etc.), dan moet er een bewerkersovereenkomst worden gesloten.

Voorbeeld: het gebruik van een financiële adviestool of CRM-systeem in de cloud. Als een systeem wordt gebruikt, maar dat systeem lokaal draait bij de financieel dienstverlener, dan hoeft er geen bewerkersovereenkomst te worden gesloten.
Bij een bewerkersovereenkomst zijn er twee partijen: een verantwoordelijke en een bewerker. Wanneer er sprake is van een van beide partijen, wordt hierna besproken.

Wanneer ben ik als financieel dienstverlener verantwoordelijke?
De bewerkersovereenkomst kent twee partijen: de verantwoordelijke en de bewerker.

De *verantwoordelijke* is degene die de persoonsgegevens initieel heeft verzameld van klanten en, zoals de wet zegt, het doel en de verwerking van de persoonsgegevens kan bepalen.

De *bewerker* is degene die in opdracht van de verantwoordelijke persoonsgegevens verwerkt.

Als er door een financieel dienstverlener gebruik wordt gemaakt van een softwarepakket in de cloud, zal de financieel dienstverlener in de regel de verantwoordelijke zijn. De leverancier van het softwarepakket is dan in het algemeen de bewerker. Dat hij de verantwoordelijke is, heeft bepaalde consequenties.
Het is bijvoorbeeld aan de verantwoordelijke om zorg te dragen voor een bewerkersovereenkomst. Hierna wordt verder ingegaan op de verplichtingen die rusten op de verantwoordelijke.

Wanneer ben ik als financieel dienstverlener bewerker?
Een financieel dienstverlener zal in de regel geen bewerker zijn. De financieel dienstverlener verzamelt gegevens van klanten om bepaalde diensten te leveren aan de klant. Daarmee is de adviseur eigenlijk altijd verantwoordelijke. Er kunnen zich echter situaties voordoen waarin de financieel adviseur wel als bewerker kan worden gezien.

Als een financieel dienstverlener bijvoorbeeld bepaalde werkzaamheden uitbesteedt aan een ander advieskantoor, dan is laatstgenoemde bewerker. In een dergelijk geval zal ook een bewerkersovereenkomst moeten worden gesloten tussen partijen.

Welke verplichtingen heeft mijn kantoor bij het verwerken van persoonsgegevens?
Als er persoonsgegevens worden verwerkt door uw kantoor, zijn er een aantal vereisten waar het kantoor rekening mee moet houden.

Toestemming
Als een kantoor persoonsgegevens van een klant wil verwerken, moet de klant daarvoor ondubbelzinnige toestemming hebben verleend. Een uitzondering daarop is het verwerken van persoonsgegevens in het kader van een overeenkomst met de klant, bijvoorbeeld om hypotheek advies te verlenen. In dat geval hoeft geen toestemming te worden gevraagd.

Informeren klant
De klant moet worden geïnformeerd over de wijze waarop met zijn persoonsgegevens wordt omgegaan en welke rechten de klant heeft met betrekking tot zijn gegevens. Het informeren geschiedt via de website van het kantoor en/of een privacyverklaring die wordt overhandigd bij het aangaan van de opdracht tot dienstverlening.

Beveiliging
De persoonsgegevens moeten op een adequate manier worden beveiligd. De mate van beveiliging hangt af van het soort gegevens dat wordt verwerkt en de hoeveelheid. Daarnaast hangt de soort beveiliging af van de huidige beschikbare technologieën. De maatstaf adequaat verandert dus continu.

Bij een financieel dienstverlener worden vaak grote hoeveelheden (bijzondere) persoonsgegevens verwerkt. Het is daarom zaak om goed te kijken naar de beveiliging van computers waarmee die informatie bereikt kan worden.

Bewerkersovereenkomst
Daarnaast geldt, zoals gezegd, de verplichting om met derden die de gegevens bewaren of bewerken in opdracht van uw kantoor, een bewerkersovereenkomst aan te gaan.

Welke verplichtingen heeft mijn kantoor bij het inschakelen van een bewerker?
Als gebruik wordt gemaakt van een bewerker, zoals een softwareleverancier, moet door het kantoor dat de klantgegevens verwerkt in de online tool van de leverancier, een bewerkersovereenkomst worden gesloten met de leverancier.

In die bewerkersovereenkomst wordt vastgelegd welke persoonsgegevens aan de softwareleverancier worden 'toegezonden'. Onder toezenden kan ook vallen het zelf invoeren van persoonsgegevens in de online software van de leverancier. Die gegevens worden dan alsnog opgeslagen in de cloud van de leverancier en dus door die partij verwerkt. In de overeenkomst wordt ook afgesproken hoe de persoonsgegevens worden beveiligd, zodat het kantoor dat ze in de cloud van de leverancier opslaat, zeker weet dat de gegevens ook daar op een adequate manier worden beveiligd.

De overeenkomst moet ook voorzien in een bepaling waarin wordt bepaald hoe er wordt gehandeld als er een datalek is bij de leverancier. Bij een datalek zal het kantoor dat de gegevens verzamelt, bij de Autoriteit Persoonsgegevens namelijk binnen 72 uur melding moeten maken van het lek. Na een (mogelijk) datalek zal het kantoor daarom snel op de hoogte moeten worden gebracht.

Wat zijn de gevolgen indien ik niet aan de wettelijke eisen voldoe?
Het orgaan dat toezicht houdt op de naleving van de Wbp, is de Autoriteit Persoonsgegevens. De toezichthouder heeft de bevoegdheid om boetes op te leggen aan bedrijven die de Wbp overtreden, ook kunnen zij naar aanleiding van berichten die hen bereiken een onderzoek instellen naar de werkwijze van een organisatie.

Naast de gevolgen die het niet naleven van de wet- en regelgeving met betrekking tot privacy kan hebben in verband met boetes of onderzoeken, kan een schending civielrechtelijke gevolgen hebben. Als persoonsgegevens van klanten op straat komen te liggen door het niet adequaat beveiligen van die gegevens, kan een klant het bedrijf dat de gegevens niet goed heeft beveiligd aanspreken.

Tot slot kunnen dergelijke gebeurtenissen slecht zijn voor de reputatie van het kantoor. Een klant zal niet graag haar gegevens achterlaten bij een bedrijf dat bekend staat om een groot datalek.

Waar kan ik meer informatie vinden?
Meer informatie over de Autoriteit Persoonsgegevens is te vinden op hun site, www.autoriteitpersoonsgegevens.nl. Daar is ook meer informatie te vinden over de privacywetgeving en de gevolgen voor uw bedrijfsvoering.