Wet bescherming persoonsgegevens en datalekken

Inleiding

De Wet bescherming persoonsgegevens (Wbp) is met ingang van dit jaar aangescherpt en onder meer aangevuld met een meldplicht in het geval van incidenten rond de beveiliging van persoonsgegevens. Heeft u personeel? Of legt u persoonsgegevens van cliënten vast? Dan is het voor u belangrijk om een aantal zaken rond de vastlegging daarvan goed te regelen en u bewust te zijn van de situatie waarin een meldplicht van toepassing is. De nieuwe Autoriteit Persoonsgegevens is verantwoordelijk voor de naleving van de nieuwe regelgeving en kan forse boetes opleggen.

Welke persoonsgegevens moet ik beschermen?

Persoonsgegevens zijn gegevens die ofwel direct over een natuurlijk persoon gaan, ofwel naar deze persoon te herleiden zijn. Naast de voor de hand liggende gegevens als naam, adres, geboortedatum en -plaats, en BSN-nummer is veel meer informatie te kenmerken als herleidbaar naar een persoon, zoals een e-mailadres, telefoonnummer, ziektekostenverzekeringsnummer, kentekengegevens en zelfs IP-adressen. U hebt de plicht om zorgvuldig met deze gegevens om te gaan.
De belangrijkste uitgangspunten hierbij zijn:

1) de persoonsgegevens worden uitsluitend gebruikt voor de uitvoering van de betreffende opdracht die u van de cliënt(en) heeft gekregen;
2) persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk;
3) u draagt zorg voor de geheimhouding van de verkregen persoonsgegevens.
   Denk aan organisatorische maatregelen rond beveiliging van het pand en de beveiliging rond uw ICT-structuur maar bijvoorbeeld ook geheimhoudingsbepalingen in de arbeidscontracten met uw personeel.

Wat is een datalek en wanneer moet ik die melden

Een incident waarbij er onverhoopt sprake is van toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is, wordt een datalek genoemd. De ernst van een datalek hangt af van de omvang van het lek, de aard van de betrokken gegevens en de kans dat een lek ook daadwerkelijk tot schade zal leiden.
Een datalek moet (onverwijld en zo mogelijk binnen 72 uur) worden gemeld aan de
Autoriteit Persoonsgegevens als het lek leidt of kan leiden tot een aanzienlijke (kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het datalek moet daarnaast ook worden gemeld aan de betrokken persoon indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Moet ik afspraken maken met derden die toegang hebben tot de persoonsgegevens die ik vastleg?

Soms hebben ook derden toegang tot persoonsgegevens die onder uw verantwoordelijkheid worden vastgelegd; de wet noemt hen ‘bewerkers’. Denk hierbij aan leveranciers van online softwareapplicaties maar ook aan uw systeembeheerder, ingeschakelde deskundigen, stagiaires, enzovoorts. Met de betreffende personen en/of organisaties moet u regelen dat ook zij vertrouwelijk en overigens zorgvuldig met de betreffende persoonsgegevens omgaan en ook dat zij u zo spoedig mogelijk zullen inlichten als er bij hen sprake is geweest van een datalek. Als primaire verantwoordelijke voor de betreffende persoonsgegevens bent u namelijk ook verantwoordelijk voor de meldingen van incidenten rond gegevens die bij bewerkers plaatsvinden.
Het kan zijn dat bovengenoemde partijen deze bepalingen al hebben opgenomen in de overeenkomst die ze met u zijn aangegaan, maar anders zult u ze nog expliciet moeten vragen dit aan u te verklaren via bijvoorbeeld een aanvulling op die overeenkomst.