PROTOCOL DATALEKKEN DORPSHUIS 'T KLOOSTER IN BAVEL

(zoals vastgesteld op 30 januari 2019)

Datalek

Onder een datalek wordt verstaan een gebeurtenis, waarbij sprake is van een inbreuk op de beveiliging van persoonsgegevens die door Dorpshuis 't Klooster in Bavel worden verwerkt, in die zin dat deze persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking (zoals een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop, een inbraak in een databestand door een hacker of het ten onrechte verstrekken van persoonsgegevens aan derden).

Melding binnen de organisatie

Indien zich een datalek heeft voorgedaan, moet dit per omgaande worden gemeld aan het bestuur.

Melding aan de Autoriteit Persoonsgegevens

Het bestuur bepaalt zo spoedig mogelijk of het datalek moet worden gemeld aan de Autoriteit Persoonsgegevens.

Het bestuur is verplicht deze melding aan de Autoriteit Persoonsgegevens te doen indien sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Dat is het geval indien één van de volgende situaties aan de orde is:

a. persoonsgegevens van gevoelige aard zijn gelekt, namelijk:
   I. bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp:
      - betreffende iemands levensovertuiging of godsdienst, ras, politieke gezindheid, gezondheid seksuele leven, lidmaatschap van een vakvereniging,
      - strafrechtelijke persoonsgegevens,
      - persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag, of
   II. persoonsgegevens die anderszins van gevoelige aard zijn, waaronder:
      - gegevens over de financiële of economische situatie van betrokkene,
      - gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene,
      - gebruikersnamen, wachtwoorden en andere inloggegevens,
      - gegevens die kunnen worden misbruikt voor (identiteits-)fraude,
      - gegevens uit DNA-databanken, gegevens waaruit een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen,
b. de aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen, waarbij van belang is of:
   I. het om veel persoonsgegevens per persoon of om gegevens van grote groepen gaat,
   II. de beslissingen, die op basis van de verwerkte persoonsgegevens worden genomen, ingrijpend zijn,
   III. de persoonsgegevens binnen ketens worden gedeeld,
   IV. het gaat om persoonsgegevens van kwetsbare groepen.

Tijdstip van melding aan de Autoriteit Persoonsgegevens
Indien het bestuur vaststelt dat de verplichting bestaat het datalek te melden, gebeurt dit onverwijld en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Zulks met dien verstande dat het bestuur enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen.
Het bestuur maakt voor de melding gebruikt van een webformulier van de Autoriteit Persoonsgegevens.

Melding aan betrokkene
Het datalek moet onverwijld door het bestuur worden gemeld aan de betrokkene wiens persoonsgegevens in het geding zijn, waarbij de betrokkene moet worden geïnformeerd over de aard van de inbreuk, de contactgegevens van de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen, en voorts de maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken.
Het bestuur mag enige tijd nemen voor nader onderzoek zodat de betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd.
Melding aan de betrokkene kan achterwege blijven:

- indien er passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens onbegrijpelijk en ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, bijvoorbeld door adequate encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code),
- het onwaarschijnlijk is dat het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene: als persoonsgegevens van gevoelige aard zijn gelekt, moet sowieso worden gemeld,
- er andere zwaarwegende redenen zijn om de melding aan de betrokkene achterwege te laten.

Vastleggen van gegevens
Het bestuur houdt een overzicht bij van alle datalekken die onder de meldplicht vallen. Dit overzicht wordt aangehouden voor een periode van vijf jaar.