LEGAL UPDATE

Boete AP aan OLVG vanwege onvoldoende beveiligingsmaatregelen

Datum: 12 februari 2021

Inleiding
De Autoriteit Persoonsgegevens ('AP') heeft op 11 februari 2021 openbaar gemaakt dat zij op 26 november 2020 een boete van €440.000,- heeft opgelegd aan Stichting OLVG ('OLVG'), omdat OLVG onvoldoende beveiligingsmaatregelen zou hebben getroffen op grond van de Algemene Verordening Gegevensbescherming ('AVG'). Zo zou OLVG ten onrechte geen tweefactor authenticatie gebruiken bij het vaststellen van de identiteit van een gebruiker en daarnaast onvoldoende hebben gecontroleerd welke medewerker wanneer welk dossier heeft ingezien. Het volledige boetebesluit leest u hier.

De door de AP gehanteerde overwegingen bevatten opvallende gelijkenissen met de overwegingen voor de boete die zij in juni 2019 aan het HagaZiekenhuis heeft opgelegd. Onze legal update over de boete aan het HagaZiekenhuis leest u hier.

Juridisch kader
Ingevolge artikel 32 lid 1 AVG dient de verwerkingsverantwoordelijke (in dit geval OLVG), rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij de beoordeling van het passende beveiligingsniveau wordt op basis van lid 2 met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig. De AP acht het in de onderliggende kwestie van belang dat OLVG op grote schaal (van circa 500.000 patiënten) gevoelige gegevens verwerkt.

Schending AVG door OLVG
Ten eerste heeft de AP geoordeeld dat OLVG ten onrechte geen gebruik maakte van zogenaamde tweefactor authenticatie. Binnen het ziekenhuis konden de medewerkers toegang krijgen tot elektronische patiëntdossiers door een gebruikersnaam en wachtwoord in te voeren. Er werd volgens de AP geen gebruik gemaakt van een andere tweede factor, zoals een pas of token. Een dergelijke beveiligingsmaatregel is volgens de AP passend, gelet op de stand van de techniek en de daarmee gepaarde uitvoeringskosten. Daarnaast neemt de AP in aanmerking dat algemeen geaccepteerde beveiligingsstandaarden, zoals NEN-normen in de zorg, tweefactor authenticatie voorschrijven.

Voorts heeft OLVG in haar eigen logging beleid opgenomen dat alle activiteiten van gebruikers, systemen en informatiebeveiligingsgebeurtenissen in logbestanden worden vastgelegd. In het beleid zijn incidentele controles en steekproeven opgenomen. De AP heeft vastgesteld dat OLVG veel minder steekproeven heeft uitgevoerd en daarmee haar eigen logging beleid niet heeft nageleefd. Bovendien zijn de controles volgens de AP evident onvoldoende om te kunnen spreken van een passend beveiligingsniveau. De NEN-normen, waarin regelmatige logging wordt voorgeschreven, is volgens de AP niet door OLVG nageleefd.

De boete
De boetebandbreedte voor dergelijke overtredingen is door de AP in haar boetebeleidsregels vastgesteld op €120.000,- tot €500.000,-. De basisboete bedraagt €310.000,-. De AP is uitgegaan van deze basisboete en heeft twee aanleidingen gezien om deze boete te verhogen, om zo tot een totale

boete van €440.000,- te komen. Aanleidingen om de boete te verhogen waren de aard, de ernst, de omvang en de duur van de inbreuk en de nalatige aard van de inbreuk. Het betreft namelijk een grote hoeveelheid zeer gevoelige informatie, welke voor lange duur onnodig extra risico heeft gelopen op onder andere onbevoegde toegang.

Het OLVG gaat niet in bezwaar of beroep tegen de boete van de AP en heeft inmiddels verbeteringen doorgevoerd.

Belang voor de praktijk
Uit deze zaak blijkt dat de AP de passendheid van beveiligingsmaatregelen toetst aan het eigen beleid van de onderneming en aan sectorspecifieke beveiliggingsstandaarden. In de praktijk zien we vaker dat ondernemingen in beleid hoge standaarden opnemen om persoonsgegevens te beschermen. Echter, indien dit beleid in de praktijk niet of nauwelijks uitvoerbaar blijkt, kan dit nadelig uitpakken voor de onderneming, zoals ook in deze zaak. Het verdient om die reden aanbeveling om in het beleid van uw onderneming realistische doelstellingen op te nemen die ook daadwerkelijk kunnen worden nageleefd. Dit beleid dient concrete handen en voeten te geven aan de open normen in de AVG en de algemene beveiligingsstandaarden binnen uw sector. Bovendien raden we aan om de governance binnen uw organisatie zodanig in te richten dat beleid ook daadwerkelijk wordt nageleefd in de praktijk.

Indien u vragen heeft over het opstellen van een beleid voor de bescherming van persoonsgegevens binnen uw organisatie of over de privacy governance binnen uw organisatie, dan kunt u contact met ons opnemen.

Dit is een Legal Update van Elze 't Hart.

Voor meer informatie:

Elze 't Hart
+31 30 25 95 580
elzethart@vbk.nl