COLUMN

Tekst **Martijn Kortier**

Martijn Kortier is advocaat intellectuele eigendom, ict-recht en privacy bij Elferink & Kortier Advocaten

Vergeet beveiliging niet!

Ons leven speelt zich steeds meer digitaal af. Daarmee worden we steeds kwetsbaarder. Kwetsbaarder voor afpersing, kwetsbaarder voor *phishing*, maar ook kwetsbaarder voor identiteitsdiefstal. Eind 2020 was er een ingrijpend datalek bij de gemeente Hof van Twente. Grote hoeveelheden data van inwoners van deze gemeente werden buitgemaakt en/of gewist. Terwijl de gemeente enorme kosten moet maken om de systemen te herstellen en beveiligen, is de echte impact voor betrokkenen nog steeds niet duidelijk. Het wachtwoord Welkom2020 was eenvoudig te kraken. Dat roept de vraag op wat nu afdoende beveiligingsmaatregelen zijn die men vanuit het perspectief van privacy zou moeten treffen. Wanneer is iets voldoende beveiligd?

De Algemene Verordening Gegevensbescherming (AVG) is in het leven geroepen om de privacy van individuen te beschermen. Deze Europese privacywet moet onder meer bewustwording vergroten bij omgang met privacygevoelige gegevens. Bovendien is men op grond van deze wet verplicht om datalekken te melden. De AVG voorziet ook in regels voor passende technische en organisatorische beveiligingsmaatregelen. Passend is een open norm. Wat in het ene geval passend is, is dat niet in het andere geval. En dat is nu precies de bedoeling. Gezondheidsgegevens zullen beter beveiligd moeten worden dan de ledenadministratie van de plaatselijke vereniging van postzegelverzamelaars. Daar ligt een verantwoordelijkheid voor degene die de gegevens verwerkt. De te treffen beveiligingsmaatregelen moeten zowel technisch als organisatorisch van aard zijn. Met dat laatste kan bijvoorbeeld worden gedacht aan cameratoezicht, het afsluiten van bepaalde ruimtes, toegang op basis van rollen, *logging*, maar ook aan een *clean desk policy*. Bovendien moet men principes van *privacy by design* en *privacy by default* toepassen. Dat betekent vrij vertaald: bij het ontwerp van producten en diensten moet men rekening houden met de privacybeschermingsbeginselen. Bovendien moet als uitgangspunt de privacy-impact in alle gevallen zo min mogelijk zijn. Uiteraard geldt: de beveiligingsmaatregelen moeten *state of the art* zijn.

De Autoriteit Persoonsgegevens (AP) legt de komende jaren bij haar toezichttaak extra nadruk op drie focusgebieden: datahandel, digitale overheid en artificiële intelligentie en algoritmes. Als u een archief beheert voor een overheidsinstelling, betekent dit dat ook uw (digitale) archief op extra aandacht van de toezichthouder mag rekenen. De verantwoordelijkheid voor privacygevoelige data houdt immers niet op bij de archivering. Zorg er daarom voor dat uw archief voldoende passende maatregelen treft voor de bescherming van de gegevens. Doet u dat niet of onvoldoende, dan kunt u naast boetes, ook een hele hoop (publicitaire) ellende verwachten.