Wat is GDPR?

GDPR staat voor ‘General Data Protection Regulation’. In het Nederlands heeft men het over AVG of ‘Algemene Verordening Gegevensbescherming’, in het Frans ‘Règlement Général sur la Protection des Données’ of ‘RGPD’. Deze Europese regelgeving vervangt de Data Protection Directive 95/46/EC uit 1995.

Waarom GDPR?

Het is de bedoeling om de privacy van de burger beter te beschermen, en daarbij uniforme regels vast te leggen voor de hele EU. Enerzijds krijgt de burger meer controle over hoe zijn persoonlijke gegevens gebruikt worden. Anderzijds legt GDPR een duidelijke wettelijke structuur vast, een standaard die in heel Europa geldt, zodat bedrijven weten hoe zij moeten handelen om de privacy te waarborgen.

Op wie is GDPR van toepassing?

Elke organisatie, elk bedrijf, elke overheid die persoonlijke data van Europese burgers verzamelt en verwerkt, moet GDPR toepassen, ongeacht het land waar het bedrijf of de organisatie gevestigd is. Een Amerikaans bedrijf dat werkt met data van Europese gebruikers moet zich dus ook aan deze regels houden. Uiteraard is dus ook ons bedrijf onderworpen aan GDPR.

Belangrijk hierbij is de definitie van wat persoonlijke data zijn. De regelgeving spreekt over PII of Persoonlijk Identificatie Informatie. Dat is niet alleen uw naam, adres, nummer identiteitskaart, Rijksregisternummer, geboortedatum, maar ook digitale data zoals locatie, IP-adres, cookiegegevens, RFID-tags. Gegevens over gezondheid vallen hier ook onder, evenals genetische, biometrische, raciale, etnische data, seksuele geaardheid en politieke opinie.

Wat bepaalt GDPR concreet?

Kort samengevat zijn dit de principes:

- **Het verzamelen van data**, zowel online als offline:
  - De gebruiker moet uitdrukkelijk toestemming geven. Bijvoorbeeld geen vooraf aangevinkte vakjes (opt-out) meer om een nieuwsbrief of commerciële meldingen te ontvangen, maar de gebruiker die zelf het vakje moet aanvinken (opt-in).
  - Op bovenstaand principe bestaan evenwel een aantal uitzonderingen: verwerking van persoonsgegevens is mogelijk zonder toestemming wanneer dit nodig is voor de uitvoering van een contract met de gebruiker, het vervullen van een wettelijke plicht, een taak van openbaar belang of de bescherming van vitale belangen van de gebruiker of andere natuurlijke personen.
  - De data-verzamelaar moet uitdrukkelijk vermelden welke data verzameld worden, en met welk doel.
  - De verzamelde data mogen enkel voor dit doel gebruikt worden, en voor een periode die strookt met dat doel.

- **Het bewaren van data**
  - Data moet je bewaren volgens een systeem dat erop gericht is de data te beschermen en de privacy ervan te waarborgen.
  - Een eventuele inbreuk op de veiligheid van de data moet binnen de 72 uur gemeld worden.
  - De gebruiker heeft recht op inzicht: hij moet toegang kunnen krijgen tot de gegevens, die kunnen inzien, eventueel verbeteren, laten verwijderen, maar ook kunnen overdragen. Het bedrijf moet een elektronische kopie kunnen voorleggen van zijn privaat bestand.
  - De gebruiker moet ook op elk moment zijn toestemming weer kunnen intrekken.

- **Het toezicht op deze data:**
  - Bedrijven met meer dan 250 personeelsleden, moeten een **Data Protection Officer** benoemen, die toezicht houdt op het correcte uitvoeren van de GDPR-regulering. Nikon Metrology heeft dus geen verplichting om een Data Protection Officer te benoemen, behalve dan in Duitsland omwille van de lokale regelgeving.
  - In de verschillende lidstaten zullen speciale controleorganisaties (**Supervisory Authority**) belast worden met de controle op de GDPR-compliance. In België werd deze bevoegdheid toevertrouwd aan de Privacycommissie.

- **Het overdragen van data** naar organisaties buiten de EU mag enkel als die organisaties kunnen aantonen dat ook zij voldoen aan de GDPR-regels.

Meer informatie over GDPR kan u terugvinden op onze website en op SharePoint.

Leuven, 21 mei 2018

K. Van der Elst

General Counsel