What is GDPR?

GDPR stands for ‘General Data Protection Regulation’. This European regulation replaces the Data Protection Directive 95/46/EC from 1995.

Why GDPR?

The purpose is to better protect citizens privacy and to set uniform regulations for the entire EU. On the one hand, citizens will have more control on the use of their personal data. On the other hand, the GDPR will set up a clear legal structure, a standard for Europe, so that companies know how to act in order to guarantee the privacy.

To whom does GDPR apply?

Every organisation, every company, every government that collects and processes personal data of European citizens, has to comply with GDPR, regardless of where the company or organization is located. An American company that processes data of European users also has to comply with these rules. Obviously also our company is subject to GDPR.

It is however important to define what personal data are. The regulation mentions PII or Personal Identification Information. That is not only your name, address, identity card number, national registration number, birth date, but also your location, IP address, cookies, RFID-tags. Data on your health are also covered, as well as genetic, biometric, racial, ethnic data, sexual preference and political opinion.

What exactly does GDPR regulate?

In short, these are the principles:

- **The collection of data**, online as well as offline:
  - The user must give explicit permission. I.e. no more pre-checked boxes (opt-out) to a newsletter or to receive commercial messages, but the user who must check the box himself (opt-in).
  - There are however a few exceptions to the above principle: processing of personal data is possible without consent when so required for the performance of a contract with the user, for fulfilling a legal obligation, a task of public interest or for the protection of vital interests of the user or other natural persons.
  - The data collector must specifically state which data are collected, and for what purpose.
  - The collected data may only be used for this purpose, and for a period that is consistent with that purpose.

- **The storage of data**
  - Data have to be saved under a system that is designed to protect the data and to ensure the privacy.
  - Any breach of security of the data must be reported within 72 hours.
  - The user has right to insight: he must be able to access the data, to consult, if necessary to correct, to have it removed, but also be able to transfer. The company must be able to submit an electronic copy of his private file.
  - The user must also be able to revoke its permission at any time.

- **Monitoring these data:**
  - Companies with more than 250 staff, must appoint a **Data Protection Officer**, who will supervise a correct execution of the GDPR-regulation. Nikon Metrology has no obligation to appoint a Data Protection Officer, except in Germany because of local regulations.
  - In the different member states special supervising organisations (‘**Supervisory Authority’**) will be appointed to control ‘ GDPR-compliance. In Belgium, this supervision authorisation was given to the Privacy Commission.

- **Transfer of data** towards organisations outside the EU is only allowed if these organisations can prove they comply with the GDPR regulations.

You can find more information on GDPR on our website and on SharePoint.

Leuven, 21st May 2018

K. Van der Elst

General Counsel