The AVG stipulates that data breaches must be reported to the Dutch Data Protection Authority within 72 hours immediately, unless it is unlikely that the data breach will lead to a high risk for the rights and freedoms of the data subjects. In addition, the data breach must also be reported to the data subjects if it is likely to entail a high risk for the rights and freedoms of those involved.

This protocol data breach is made to answer the question whether there is a data breach and whether it should be reported.

What is a data breach?
In the case of a data breach, personal data are exposed to loss or unlawful processing. It could be a lost USB stick or a stolen laptop with personal data, but also a leak in a data system or accidentally provided access to data to persons or authorities that should not have access to it. Sending an e-mail to an address file in which all e-mail addresses are visible to everyone is also a data breach.

Contact person for reporting a data breach
The contact persons for reporting a data breach at Muller Dordrecht are:
- Office manager;
- CEO.

The notifications can be submitted via +31(0)78-6392000.
Employees within the organization should be aware that if there is a data breach, they must report this data leak immediately (the same day) to the designated Contact Person, so that they can report the data breach to the Dutch Data Protection Authority in a timely manner. They should be familiar with the step-by-step plan included in this protocol.

The step-by-step plan for a data breach
1. Immediately after an employee discovers or learns that there may be loss or unlawful processing of personal data within Muller Dordrecht, he reports this to the contact persons.
2. The contact person decides whether there is a (possible) data breach and whether this (possible) data breach must be reported to the Dutch Data Protection Authority and / or to the data subjects. If possible, the data breach is stopped and action is taken to limit any consequences.
3. The contact person is responsible for reporting to the Dutch Data Protection Authority and / or the parties involved. The employee is not permitted to report the (possible) data breach to the Dutch Data Protection Authority and / or the parties involved.
4. If the employee does not agree with the decision of the contact person to report the (possible) data breach or not to the Dutch Data Protection Authority and / or those involved, he can contact the CEO. If necessary, the data leak process will be evaluated and improved.