5. DATA PROTECTION

At HMC, we endorse internal and external rules that safeguard a responsible way of working. As an HMC employee, you also carry this responsibility. You are therefore expected to act in line with our policies and applicable data protection laws.

What is data protection?

Data privacy or data protection concerns the collection, protection and distribution of personal data or confidential information about organizations.

Personal Data

Personal data means any data relating to an identifiable natural person. This includes information such as dates of birth, social security numbers, passwords, bank account numbers or data concerning health, ethnic origin, political opinions, religious beliefs or sexual orientation. Leaking personal data may result in identity theft or fraud.

We are committed to protecting the privacy rights of our employees and everyone with whom we do business. We feel it is important for everyone that they can trust their (personal) data is safe with us. Personal data will be saved only for the period necessary and to the extent allowed by law.

Confidential information

Confidential information is all non-public, business-related information, such as information that might be of use to competitors. Examples include information on business plans, trade secrets, intellectual property or operations that are not known to the general public or competitors. Disclosing confidential information could result in losing competitive advantage or losing intellectual property rights.

During our daily work, we gain and produce information that is vital to our business. Such

information may, however, also be valuable for competitors and others. Therefore, we commit to protect information created by us, or given to us, to ensure appropriate confidentiality.

Points of attention

The following is a list of possible warning signals that may arise during the course of your work. The list is not intended to be exhaustive and is for illustrative purposes only.

Pay special attention when:

- You work with personal data.
- You share confidential company information outside HMC.
- You are transferring personal data to another party or outside the country where the data originates from.
- You receive a suspicious email (e.g. you are requested to provide personal information or to make payments).

EXAMPLES

Examples of inadequate data protection

- You leave a CV containing personal data in a common area.
- You give your HMC username and password to someone else.
- You leave your laptop unattended during travelling.
- You share confidential company information (including on-the-job photos) with (social) media without prior written approval of the HMC Communications Officer.
- You forward confidential information to your personal email account or use your personal email to conduct any HMC business.
- You use unauthorized cloud storage/data transfer services to store or transfer information.

DATA PROTECTION

KEY TAKEAWAYS

- Personal data may be processed on the basis of a number of grounds. When you process personal data ensure that it is accurate, relevant and not excessive in relation to your needs. Further, make sure that the personal data is protected.
- When sharing confidential information with external parties, make sure that the recipient is authorized to receive the information and understands how the information should be used.
- Please consider using password protection if you use confidential information in Word or Excel.
- Do not leave documents unattended on your desk.
- Please note that failure to comply with this policy can be reason for disciplinary action.

What does this mean for third parties?

At HMC, we want to make sure third parties are reputable, capable and commercially reliable companies. Therefore:

- We expect all our business partners to act in line with our data protection policy and applicable laws.
- If we feel it is necessary, we monitor their behavior and end our relationship with any third party who fails to comply with this policy.

Do you have any questions about this topic?

We encourage you to contact the Ethics & Compliance department. The contact details can be found on the Ethics & Compliance intranet site.

Speak up!

If you think that a security breach or leakage of (personal) data has occurred, immediately inform the Ethics & Compliance department and the Manager Information Systems. If you suspect any other misconduct, please take a look at the Reporting Policy to see what you can do.