27. Januar 2022

# YPOG Briefing:
## Non-Disclosure Agreements

Berlin, January 27, 2022 | Dr. Benedikt Flöter and Leon Feldman

## Overview

Non-Disclosure Agreements ("NDA") are used to protect know-how, trade- and business secrets that are to be disclosed to negotiating partners and have significant economic value yet are not protected by copy- or patent rights. Proper drafting of the NDA ensures the confidentiality of such information. The NDA's requirements are largely determined by the purpose of the information disclosure: In the run-up to transactions as well as in the subsequent due diligence process the disclosed information generally includes key company figures, customer and manufacturer contacts or the identity of key employees. In the case of strategic investments as well as joint ventures, the focus will be more on know-how relevant for the company's business operation (methods, processes, technologies, etc.). At the same time, the diligent use of NDAs is part of the cross-company trade secret compliance, which is intended not only to preserve trade secrets but also to allow their commercial exploitation. Legal benchmark for the drafting of NDAs and the trade secret compliance is the German Act on the Protection of Trade Secrets ("GeschGehG").

Three key requirements must be met to obtain trade secret protection:

## 1.

Obviously the information concerned must be **confidential**. This requires that the information or know-how in the specific composition is neither generally known nor easily accessible. The economic value of the information must lie precisely in its confidentiality.

## 2.

The company must protect the information by implementing **reasonable steps to keep it secret**. This applies even if the information is secret as a matter of fact, i.e. in the absence of any secrecy measures, there is no legal protection. The economic value of the secret determines which measures are reasonable. The implementation of reasonable measures is a duty of the managing director/board of directors pursuant to sec. 43 (2) Limited Liability Companies Act / sec. 93 (2) Stock Corporation Act, the violation of which may lead to personal liability.

## 3.

Not all information can be protected, but protection requires a **legitimate interest in keeping it confidential**. In the case of commercially valuable information, generally a legitimate interest can be assumed.

To ensure that these requirements are met and evidenced in case of conflict, we recommend implementing the following six measures:

1. Create a **list of the six most important trade secrets.**

2. **Classify** these secrets based on their economic/operational value to your company.

3. **Review** existing secrecy measures and identify opportunities for optimization:

    - Restrict your employees' access to trade secrets, based on the "need to know" principle.
    - Set up organizational (access restrictions, monitoring, etc.) and technical protection measures (passwords, 2-factor authentication, IT security).
    - Create a security concept, a home office policy, and a guideline on the use of employee-owned IT hardware (BYOD).
    - Review existing employment- and other contracts for effective non-disclosure agreements and amend if necessary.
    - Use NDAs in all business relations that require the disclosure of trade secrets.

4. **Document** the implementation of these measures.

5. Schedule **employee trainings**, in particular regarding IT security (e.g., phishing emails, Trojans), the use of private devices and the use of sensitive information when working from home.

6. Appoint a **"trade secret protection officer"** who is internally responsible for trade secret protection and is point of contact for your employees.

We are happy to support you and open for further exchange.

**Your contact at YPOG:**

Benedikt Flöter
Associated Partner, Berlin

+49 30 7675975 177
+49 151 40228534
benedikt.floeter@ypog.law