TOPSOE

STATEMENT ON DATA ETHICS 2025

2025

STATEMENT ON DATA ETHICS 2025

Digitalization opens up opportunities for new and better ways of working, but it also brings new responsibilities for how we handle and protect data. We use many different technologies to process data and depend on data to deliver services and improve our products. Data is therefore a key asset for us, and we treat it with care, sensitivity, and respect.

Safeguarding our own knowledge and that of our customers is essential and requires continuous attention to data security. Ensuring that the Topsoe Group has the right measures in place to protect and process data ethically is a natural and integral part of how we do business.

Data ethics goes beyond merely complying with data protection laws. We meet legal requirements, but we also recognize that our use of data – both personal and non-personal – can pose risks to users that are not fully addressed in legislation. We handle these risks by adhering to the principles set out in our Data Ethics Policy. These principles include transparency, data quality, fairness and non-discrimination, autonomy, ethics by design, responsible data sharing, and accountability.
Cyber security is a core element of our Zero Harm activities and spans several areas, including preparations to comply with the NIS2 regulations, under which we are qualified as an "Important" entity from 2025.

Our initiatives and improvements are driven by internal, scenario-based risk assessments as well as independent external security evaluations. This enables us to concentrate on the most critical improvements and continuously benchmark ourselves against peers in our industry. During the year, we conduct mandatory cyber security awareness training with a particular focus on phishing emails, which remain the most common method used to compromise a company's security defenses.

We have also enhanced our supplier evaluations to include a comprehensive cyber security assessment. In doing so, we collaborate with our suppliers to strengthen the overall security posture across our organizations.