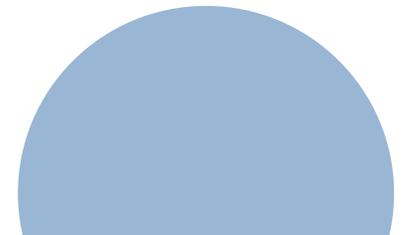
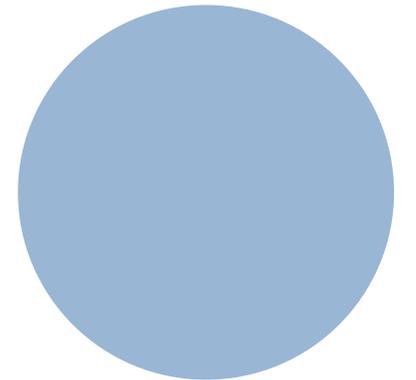
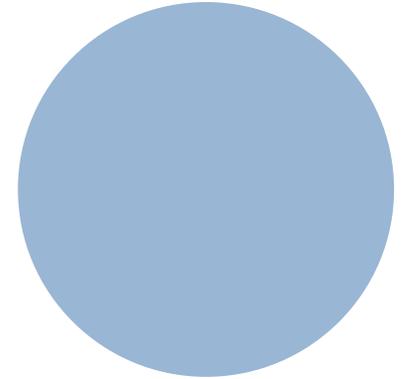


# Cybersicherheit

## Anforderungen und Verantwortlichkeiten bei Herstellern und Betreibern

7. Fachtagung Arbeitsplanung und Prävention  
Christoph Preuße (BGHM), 22.04.2021



## Zeitstrahl **Änderung der Maschinenrichtlinie**

Diskussionen  
in MWG

Erste Ideen-  
sammlung seitens  
DG GROW<sup>2</sup>

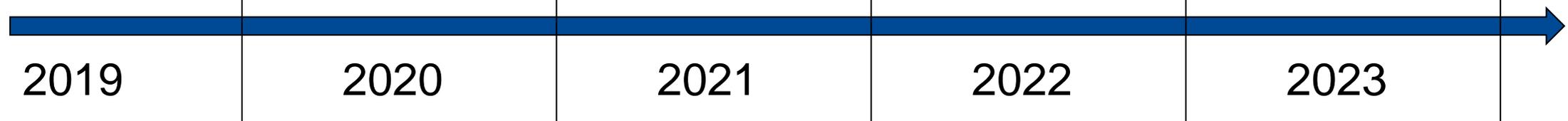
Powerpoint mit  
Änderungspunkten

2 Abfrage-  
Zeiträume

21.April:  
Erster Entwurf  
einer neuen  
Maschinen-  
verordnung

Parallel:  
Horizontale EU-  
Rechtsverordnung  
zu Cybersicherheit

???



<sup>2</sup>: GENERALDIREKTION GROW: Binnenmarkt, Industrie, Unternehmertum und KMU

## Neue MVO: Was soll geändert werden? (1)

- Schwerpunkte bei der Überarbeitung der Maschinenrichtlinie
- Anpassung an NLF
- Anhang IV
- Abgrenzung zu anderen Richtlinien, insbesondere LVD, RED, PED, AufzugsRL,
- Elektromobilität
- neue Technologien (Digitalisierung, Machine learning (AI))
- Mensch-Maschine-Kollaboration
- Form der Betriebsanleitung

## Neue MVO: Was soll geändert werden? (2)

- Schwerpunkte bei der Überarbeitung der Maschinenrichtlinie
- Gesamtheit von Maschinen
- Herstellung für den Eigengebrauch („Installer“ / “Integrator“)
- Anwendungsbereich (wesentliche Veränderung)
- unvollständige Maschinen

## Neue MVO (1) Status 21.04.2021, 13:00 Uhr

### ANNEX III

- 1.1.2 Principles of safety integration
  - (e) Functional test and description of specific functional test procedures, essential to enable it to be tested, adjusted, maintained and used safely.
- 1.2.1. Safety and reliability of control systems
  - ... Control systems of machinery products with fully or partially evolving behaviour or logic that is designed to operate with varying levels of autonomy shall be designed and constructed in such a way that:
    - (a) they shall not cause the machinery product to perform actions beyond its defined task and movement space;
    - ...
    - (g) the protective devices shall remain fully effective or give a stop command;
    - ...

## Neue MVO (2) Status 21.04.2021, 13:00 Uhr

- 1.2.1. Safety and reliability of control systems

...

Particular attention shall be given to the following points:

- For wireless control, a failure of the communication or connection or a faulty connection shall not lead to a hazardous situation.
- For autonomous mobile machinery products, the control system shall be designed to perform the safety functions by itself as set out in this section, even when actions are ordered by using a remote supervisory function.

## Neue MVO (3) Status 21.04.2021, 13:00 Uhr

### **ANNEX I HIGH-RISK MACHINERY PRODUCTS**

- ...
- 24. Software ensuring safety functions, including AI systems.
- 25. Machinery embedding AI systems ensuring safety functions.

### **ANNEX II INDICATIVE LIST OF SAFETY COMPONENTS**

- ...
- 18. Software ensuring safety functions, including AI systems.

## New Legislation Framework (NLF)

**Das Paket der NLF 2008 bekräftigt die Anwendung und Durchführung der internen Marktüberwachung.**

**Das NLF basiert auf:**

[Regulation \(EC\) 765/2008](#) VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates

[Decision 768/2008](#) BESCHLUSS Nr. 768/2008/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 9. Juli 2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates

[Regulation \(EU\) 2019/1020](#) Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011

# „White Paper on AI“



Brussels, 19.2.2020  
COM(2020) 65 final

## **WHITE PAPER**

**On Artificial Intelligence - A European approach to excellence and trust**

© Europäische Union ([www.ec.europa.eu](http://www.ec.europa.eu))

## Deutsche Position zur Implementierung von KI

„Der Hersteller muss im Rahmen der Risikobeurteilung die Grenzen der Maschine festlegen. Dies beinhaltet auch das Selbstlernen. Wenn der Hersteller jedoch die Risiken auf Grund des Selbstlern-Prozesses nicht beurteilen kann, kann er die Maschine nicht richtlinienkonform in Verkehr bringen.

Die klare Trennung zwischen gesetzlichen Bestimmungen zum Inverkehrbringen und zum Betrieb muss beibehalten werden, da sie die Verantwortung des jeweiligen Akteurs eindeutig festlegt und seit vielen Jahren erfolgreich ist.“

## **CSA: Ratschlussfolgerungen** auf Initiative der Deutschen Präsidentschaft in 12/2020:

- Commission to address in short-term cybersecurity aspects in relevant legal acts, for example acts under the New Legislative Framework (NLF), particularly Directive 2014/53/EU (Radio Equipment Directive),
- assessing the need for horizontal legislation,
- WELCOMES in this regard a discussion to explore the scope of such a legislation and its links with the cybersecurity certification framework as defined under the Cybersecurity Act (CSA),
- cybersecurity requirements should be defined in line with the relevant Union legislation, including the CSA, the NLF,
- taking utmost account of the horizontal European cybersecurity certification schemes currently being developed,
- NOTES the need to consider the adaptation of essential requirements of the respective NLF Directives, where appropriate.
- assess, where necessary, complementary sector-specific regulations that should define which level of cybersecurity should be met by the connected device to ensure that specific security and privacy requirements are put in place for such devices with higher security risks.

## Horizontaler Rechtsakt „Künstliche Intelligenz“ (1)

- **Option 3+:**  
Horizontal EU legislative instrument following a proportionate risk-based approach + codes of conduct for non-high-risk AI systems;
- **HIGH-RISK AI SYSTEMS (TITLE III)**  
two main categories of high-risk AI systems:
  - AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment;
  - other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III.

## Horizontaler Rechtsakt „Künstliche Intelligenz“ (2)

### **ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)**

- Biometric identification and categorisation of natural persons
- Management and operation of critical infrastructure
- Education and vocational training
- Employment, workers management and access to self-employment
- Access to and enjoyment of essential private services and public services and benefits
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes

## Wichtige Normungs- und Gremienarbeit zum CSA und AI

- ISO/TR 22100-4 „Sicherheit von Maschinen – Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits-(Cybersicherheits-) Aspekte;
- *ISO/TR 22100-5 „Safety of machinery - Implications of embedded Artificial Intelligence-machine learning“*;
- DIN EN ISO 11161: „Integration von Maschinen“, Smart Manufacturing implementiert  
ISO/IEC JWG 21: „Smart Manufacturing Reference Model(s)“;
- ISO/IEC JTC1 SC 42: ISO/IEC AWI TR 5469:  
“Artificial intelligence - Functional safety and AI systems“;
- Projektskizze Überarbeitung EmpfBS 1115 „Cybersicherheit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen“

## Zum Schluss

**„Weder Transhumanisten noch Posthumanisten führen die Diskussion um hochautomatisierte Systeme zum Ziel. Der Mensch muss immer und auch hier im absoluten Mittelpunkt stehen.“**

**Danke für Ihre Aufmerksamkeit.**

Christoph Preuße  
Berufsgenossenschaft Holz und Metall  
Isaac-Fulda-Allee 18  
55124 Mainz  
06131 / 802 - 18148