# Cyber Security of AI Code of Practice and Technical Standard

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# WHAT IS THE NATIONAL CYBER SECURITY CENTRE (NCSC)?

- UK's National Technical Authority on cyber security

- Part of the UK Government, but not a policy department or a regulator

- Collaborate with and provide advice to…
  - UK government departments
  - Industry (UK and global) and Institutions (such as Standards Bodies)
  - International counterparts
  - Academia, Think Tanks, Research Centres, etc
  - Wider society (aka the public)

National Cyber Security Centre

- We work to…
  - Understand the evolving cyber threat
  - Develop cyber security mitigations and publish advice/guidance
  - Reduce risk by securing and improving the resilience of public & private networks
  - Respond to significant cyber security incidents

https://www.ncsc.gov.uk/

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# SCOPE OF AI CYBER WORK

- Addressing the cyber security risks to AI
- All AI systems which includes different models, tools and technologies
- Entire lifecycle of AI
- AI supply chain, particular focus on developers and deployers



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# WHY DID WE WANT TO DEVELOP A STANDARD?

- Create international alignment on minimum security requirements for AI systems
- Drive good cyber security practices in organisations planning to and already deploying AI
- Supported by the cyber security community due to clear baseline expectations to protect systems and supported by the AI industry due to its reasonable/proportionate requirements



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# STAGES OF THE WORK

- NCSC's Guidelines for Secure AI Development
- Research outputs (risk assessment, literature reviews, organisation survey) and collaboration with other governments and in multilateral fora
- Global consultation on draft Code of Practice, technical review and publication of Code of Practice & Implementation Guide
- Development of ETSI Technical Standard and Accompanying Guide



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# GLOBAL CONSULTATION KEY STATS

- 12 workshops
- 123 responses (5 government responses, 10 from industry/trade associations and 9 membership bodies)
- 80% supported DSIT's proposed approach, 11% opposed and 9% don't know
- Support for the principles ranged from 83% to 90%
- Main overarching feedback was that stakeholders wanted more guidance on how to implement the Code


This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# MAIN CHANGES TO UPDATED CODE

- New principle on disposal and decommissioning of AI systems
- Principles now more contextualised to AI security
- Revised stakeholder groups
- Implementation Guide on how to implement the Code



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# THE NEW IMPLEMENTATION GUIDE

- The Implementation Guide was led by John Sotiropoulos (OWASP co-chair). Technical reviews were provided by DSIT, NCSC and ICO.
- The document includes detailed actions linked to examples of AI use cases to support organisations with adhering to the Code.
- We have ensured the Guide is mapped to UK and international publications for consistency.
- The Guide has been submitted to ETSI so that it can become the accompanying guide to the future standard.



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# ACTIVITY SINCE PUBLICATION OF CODE

- Further review from AI professionals and cyber security experts at ETSI
- Approval and publication of ETSI Technical Specification
- Approval and imminent publication of Accompanying Guide as a Technical Report
- Research projects (future gap analysis and mappings)
- Ongoing engagement with industry partners, international counterparts, academia and other standards bodies (CEN/CENELEC and ISO/IEC) for further consultation to upgrade TS to EN to ensure alignment of the EU AI Act
- Work with stakeholders to support future adoption of the standard inside EU market and outside EU market.



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

# WHAT IS IN THE STANDARD (TS 104 223)?

**Secure Design**

Principle 1: Raise awareness of AI security threats and risks

Principle 2: Design the AI system for security as well as functionality and performance

Principle 3: Evaluate the threats and manage the risks to the AI system

Principle 4: Enable human responsibility for AI systems

**Secure Development**

Principle 5: Identify, track and protect the assets

Principle 6: Secure the infrastructure

Principle 7: Secure the supply chain

Principle 8: Document data, models and prompts

Principle 9: Conduct appropriate testing and evaluation

**Secure Deployment**

Principle 10: Communication and processes associated with End-users and Affected Entities

**Secure Maintenance**

Principle 11: Communication and processes associated with End-users and Affected Entities

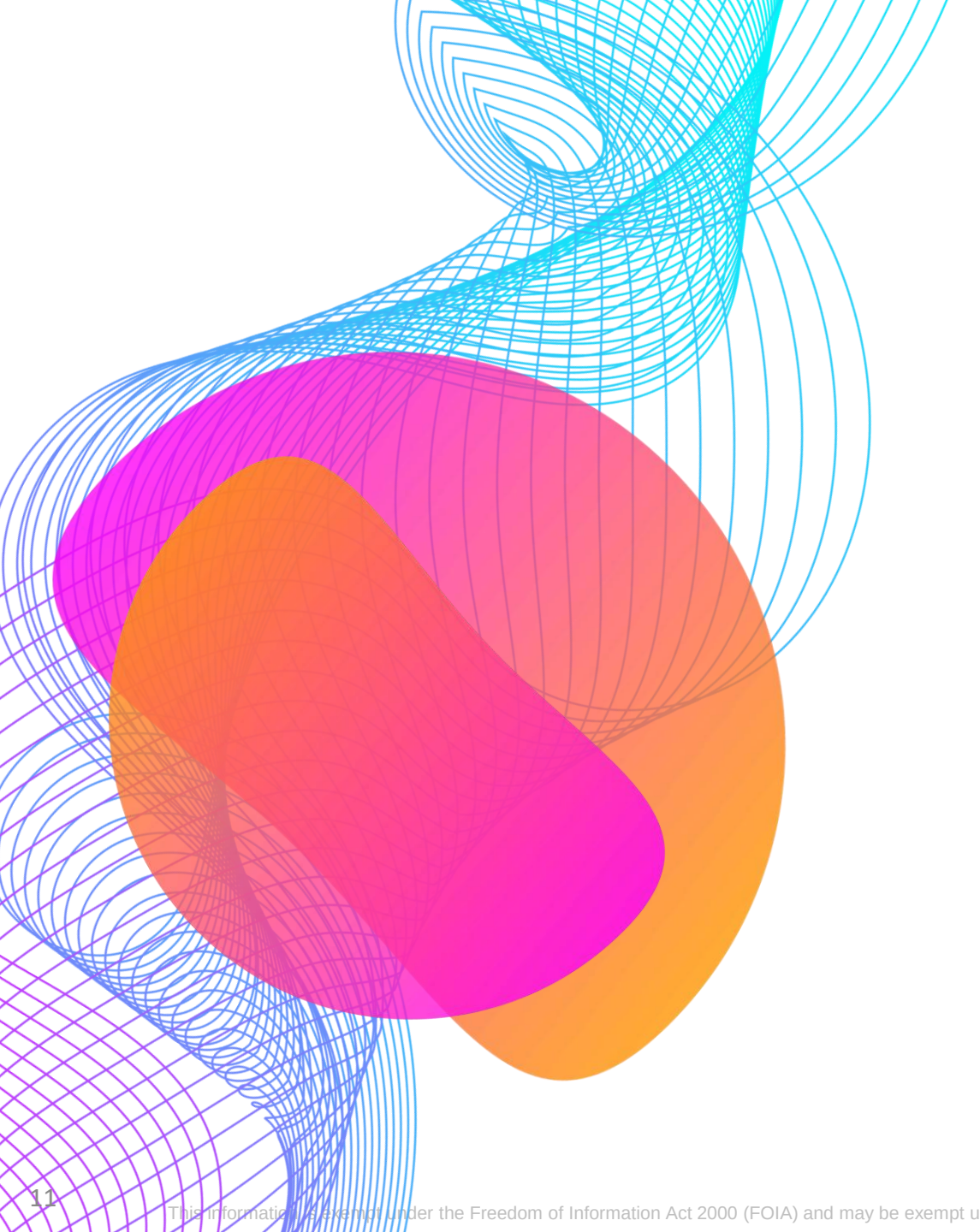
Principle 12: Monitor the system's behaviour

**Secure End of Life**

Principle 13: Ensure proper data and model disposal



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©



# Q&A



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©