# Project Specialization – cyber security

this document will include details that will needed to be considered in order to keep the product safe, as well as compliant with legislation.

## Chat gpt prompt:

what legislation will need to be considered in a program which will take a dataset from a company - which will include sales data - which will then project, using ai, considerations in a supply/ demand sort of output (for uk legislation)

## response 1:

**Data Protection & Privacy (Primary Area of Compliance)**

**UK GDPR**

The UK-specific version of the GDPR applies to any personal data, including:

- customer identifiers
- purchase histories
- customer emails or phone numbers
- business contact data if identifiable

Key duties:

- **Lawful basis for processing** (likely “legitimate interests” or “contract”).
- **Purpose limitation** — you must only use the data for agreed purposes.
- **Data minimisation** — only collect/use what is necessary for forecasting.
- **Security requirements** — appropriate technical & organisational measures.
- **Transparency** — the company must inform customers that data is used for analytics/forecasting.

**Data Protection Act 2018**

This is the UK's national implementation of GDPR. It:

- Defines exemptions and special category data handling
- Provides enforcement powers to the **ICO**
- Sets rules on automated decision-making and profiling

If your AI projections impact individuals (e.g., personalised offers), additional safeguards apply.

## Analysis:

Because the program will not deal with any personal data, this will not affect the project.

## Response 2:

**2. AI-Specific Regulation in the UK**

The UK does **not** (yet) have a single AI Act like the EU. Instead, it is taking a **sector-led, principles-based approach**.

You must consider:

**UK Government AI Regulation Framework (2024–2025)**

Principles include:

- **Safety, security, robustness**
- **Appropriate transparency**
- **Fairness and accountability**
- **Contestability and redress**

Not legally binding yet, but regulators (e.g., ICO, CMA, FCA) enforce elements through existing laws.

**ICO Guidance on AI & Data Protection**

This is effectively binding under UK GDPR. It covers:

- AI risk assessments
- Data quality requirements
- Privacy by design for AI
- Automated decision-making rules
- Fairness and mitigation of bias

**CMA Oversight (Competition and Markets Authority)**

If the AI system influences:

- pricing
- availability
- supply-side decisions

The CMA requires that:

- AI does not unintentionally collude
- pricing algorithms do not produce anti-competitive results

## analysis:

a chunk of this response which stuck out to me was the cma oversight.

Whilst the program will not have a direct affect, on pricing and availability. I believed it was worth while asking it to go into more detail about this.

"can you expand on cma oversight please"

**CMA Oversight: What You Need to Know for AI Forecasting Tools**

The **Competition and Markets Authority (CMA)** is the UK regulator that ensures businesses compete fairly and consumer markets work properly.

Even if you are not building a pricing algorithm, the CMA may still care about your AI system because **AI can unintentionally affect market competition**.

Below is the detailed breakdown.

---

**Why the CMA cares about AI used in forecasting**

The CMA has warned that AI can:

**✓ Enable or amplify anti-competitive behaviour**

For example:

- If multiple companies use similar AI tools, they may **indirectly coordinate prices or supply strategies** without explicit communication.
- AI may learn patterns that mirror price-fixing.

**✓ Lead to algorithmic collusion**

Even unintentional:

- Algorithms reacting to each other's outputs
- Systems converging on "stable" higher prices or lower supply

**✓ Harm consumers**

If an AI forecasting system leads to:

- higher prices
- limited availability
- market segmentation
- unfair commercial practices

...the CMA will intervene.

From what I gather, the cma will intervene if multiple companies collude in the use of ai to coordinate prices which where ais will then work off of each other's data. this will then cause a rise in price for the consumer which the cma is trying to counteract. From this interpretation, I believe the program will be acceptable due to the following reasons

- the ai model will not necessarily be using pricing structures to base the supply for the companies.
- The ai model will not be able to see other ai models data, even If multiple companies use our data, then the ais will work for only the company.

Later in the response it then reaffirms this by stating:

**What the CMA expects from AI systems**

**✓ 1. Clear governance and auditing**

You must ensure:

- AI outputs are *explainable*
- Risks are assessed and documented
- AI behaviour is monitored over time

**✓ 2. Competition compliance for shared tools**

If many clients use the tool:

- avoid creating "signals" or shared indicators that align strategies
- ensure outputs are **individualised** to each business
- prevent cross-client leakage

**✓ 3. No use of competitors' data**

Even aggregated benchmarks can be risky if they reflect competitors' behaviours.

**✓ 4. Human oversight**

Businesses must be able to:

- understand the recommendation
- override or challenge the AI output

## response 3:

**Cybersecurity Legislation**

**NIS Regulations (as amended by UK law)**

If the organisation is in a key sector (energy, transport, digital services), then NIS duties apply:

- Maintain cybersecurity measures

- Report relevant incidents

For most retail/consumer-facing businesses, NIS isn’t triggered unless you are a “digital service provider”.

**Computer Misuse Act 1990**

Applies generally — ensure no unauthorised system or data access occurs.

## Analysis:

Legislation that has been suggested will definitely be taken into account. conforming to this, the model will need to be password protected for each user. Following on from this, the usernames and passwords will then therefore need to be stored in compliance with GDPR.

Furthermore, its mention of NIS regulation can be disregarded due to the fact that a company will more than likely not be considered a key sector.

## References

OpenAI. (2025) *ChatGPT (version 5.1)* [Large language model]. Available at: https://chat.openai.com/ (Accessed: 24 November 2025).