VentureESG: ESG Compliance

1. Generic requirements (applicable from day 1 to most businesses)

While this list is not exhaustive, it is intended to provide initial guidance for businesses to ensure they comply with key legal standards from day one, helping to protect employees, customers, and stakeholders.

1.1 National legislation

- **Employment law**
  Examples: Minimum wage, anti-discrimination, employee benefits, and dismissal procedures
  - Employment Rights Act
  - Equality Act
- **Health and safety regulations**
  Examples: Fire safety standards, worker injury protocols, accident prevention policies
  - Health and Safety at Work Act
- **Data protection regulations**
  Examples: Regulates privacy, data security, and consent
  - Data Protection Act
- **Anti-bribery laws**
  Examples: Prevent corrupt practices and maintain compliance with ethical standards
  - UK Bribery Act
- **Taxation and corporate structure**
  Examples: Regulations that govern corporate income tax, VAT, and other business taxes as well as requirements to register a business entity (e.g., LLC, corporation, etc.)
  - Companies Act
- **Environmental regulations**
  Examples: National environmental standards and international commitments that govern waste management, emissions, or sustainability practices.
  - Environmental Protection Act
- **Consumer protection laws**
  Example: Consumer rights laws, product labelling, and advertising standards
  - Consumer Rights Act
  - Consumer Protection Act
  - General Product Safety Regulations
  - Digital Markets, Competition and Consumers Bill
  - Consumer Protection from Unfair Trading Regulations
- **Intellectual Property (IP) laws**
  Examples: Trademarks, copyrights, and patents that protect a company's intellectual property
  - Intellectual Property Act

1.2 International laws and standards

- **OECD Guidelines for Multinational Enterprises**
  - Although non-binding, these guidelines promote responsible business conduct in areas such as employment, environment, human rights, and anti-corruption for companies operating internationally
- **International Labour Organization (ILO) standards**
  - The ILO sets international standards for labour rights and working conditions that apply to companies operating globally, including minimum wage, working hours, and non-discrimination
- **International trade compliance**
  Businesses engaged in global trade must follow WTO rules on tariffs and competition, comply with export controls like the EU Dual-Use Regulation and U.S. Export Administration Regulations (EAR), as well as adhere to international sanctions from bodies like the UN and EU, especially when trading with restricted regions or entities

2. Threshold-based regulations (triggered by business size or scale)

Certain regulations only apply once a business reaches specific thresholds based on turnover, number of employees, or total assets. These are important as businesses grow in size:

- **Modern Slavery Act**
  - **Threshold:** Businesses in the UK with an annual turnover of £36m or more
  - **Requirement:** Publish a statement on actions taken to prevent slavery and human trafficking in supply chains

- **Streamlined Energy and Carbon Reporting (SECR)**
  - **Threshold:** Companies meeting at least two of the following: A turnover of £36 million+, 250+ employees, or a balance sheet total of £18 million+
  - **Requirement:** Energy and carbon emissions reporting in annual financial statements
- **Gender Pay Gap Reporting**
  - **Threshold:** UK businesses with 250 or more employees
  - **Requirement:** Written information on the company's gender pay gap, submitted to the gender pay gap service and uploaded to the company's own website
- **Energy Savings Opportunity Scheme (ESOS)**
  - **Threshold:** Companies with >250 employees or an annual turnover over £44 million and an annual balance sheet total over £38 million
  - **Requirement:** Audits of the energy used by their buildings, industrial processes and transport designed to identify tailored and cost-effective measures to save energy and achieve carbon and cost savings
- **Corporate Sustainability Reporting Directive (CSRD)**
  - **Threshold:** Companies meeting at least two of the following: 250+ employees, €40 million+ turnover, €20 million+ in total assets
  - **Requirement:** Sustainability reporting on environmental, social, and governance (ESG) factors
- **Corporate Sustainability Due Diligence Directive (CSDDD)**
  - **Threshold:** EU companies with 1,000 employees if, during a financial year, they had an annual worldwide net turnover of more than €450 million. Non-EU companies which have more than €450 million net turnover in the EU.
  - **Requirements:** Companies must identify, prevent, mitigate, and account for adverse sustainability impacts in their operations and value chains.
- **International Energy Efficiency Directive (EED)**
  - **Threshold:** Applies to large enterprises (250+ employees, turnover over €50 million)
  - **Requirement:** Conduct regular energy audits and implement energy-saving measures
- **Sustainability Disclosure Requirements (SDR)**
  - UK regulation, launched in 2023 by the UK Financial Conduct Authority (FCA), which includes rules and requirements related to sustainable investing, such as naming and marketing rules. The regulation applies to issuers of bonds and shares listed on a UK-regulated market and UK-based investment managers

3. Sector-specific requirements (vary by industry)

Sector-specific regulations address the unique challenges and risks faced by different industries. These regulations often focus on compliance, safety, and transparency in key areas like consumer protection, data privacy, and operational integrity.

3.1 B2B SaaS

- **AI Regulation:**
  - **EU AI Act**: Governs the development and use of AI systems, with a focus on transparency, safety, accountability, and ethical use of AI technologies. Applies to businesses deploying or providing AI services
  - **Proposed EU AI Liability Directive**: Addresses legal frameworks for damages caused by AI products and services, ensuring accountability for AI providers
- **Data Privacy and Security:**
  - **GDPR (EU)**: Covers the protection of personal data processed by B2B SaaS providers, including obligations around data collection, storage, and user consent
  - **US Cloud Act**: Regulates data sharing and storage across borders, with implications for SaaS providers working with US-based clients

3.2 Consumer tech

- **Influencer Marketing and Social Media:**
  - **Advertising Standards (UK CAP Code, US FTC Guidelines)**: Ensures transparency in influencer marketing, requiring disclosure of paid partnerships and endorsements
  - **Online Harms Bill (UK)**: Under review, aimed at addressing risks like misinformation, addictive behaviours, and protection of children on social apps
  - **EU Digital Services Act**: Regulates content moderation and user safety, including harmful content in consumer tech platforms
- **Mental Health and Consumer Protection:**
  - **Children's Online Privacy Protection Act (COPPA)**: Protects children's data and privacy in consumer social apps, especially regarding targeted advertising
  - **Adolescent Mental Health Risks**: Emerging regulations on peer-to-peer fashion platforms and their impact on mental health
- **Consumer Product Safety and Green Claims:**

- **Green Claims Regulations**: Regulates sustainability claims about products and services, requiring evidence of eco-friendly practices across the entire product lifecycle
    - Examples: *UK Green Claims Code*, *EU Green Claims Proposals*, *US Green Guides*
- **Consumer Product Safety (CPSIA in the US, EU General Product Safety Directive)**: Protects consumers by ensuring products are safe for use and properly labelled

3.3 Fintech

- **Anti-Money Laundering (AML) and Know Your Customer (KYC) Compliance:**
    - **Fifth Anti-Money Laundering Directive (AMLD5)**: Mandates stringent AML and KYC requirements for financial institutions, including fintech, to prevent financial crime
    - **FCA Consumer Duty (UK)**: Sets higher standards of care for consumers, requiring fintech companies to act in the best interests of customers.
- **Payment Services Regulations:**
    - **Payment Services Directive 2 (PSD2 – EU)**: Enhances consumer protection, promotes innovation, and strengthens security in electronic payments
    - **EMIR (European Market Infrastructure Regulation)**: Applies to derivatives trading and fintech companies offering such services, ensuring transparency and risk management
- **Consumer protection for investment products**
    - **MiFID II (Markets in Financial Instruments Directive II):** Enhances investor protection by improving the functioning and transparency of financial markets
    - **MiFIR (Markets in Financial Instruments Regulation):** Established uniform requirements for the transparency of transactions across the EU financial markets
    - **MiCAR (Markets in Crypto-Assets Regulation):** Introduced licensing requirements for crypto-asset service providers (CASPs), established disclosure and transparency rules for issuers, implemented consumer protection measures, and created a market abuse regime for crypto-assets

3.4 Healthtech

- **Health Data Protection:**
    - **HIPAA (US)**: Regulates the use and protection of personal health information in the US.
    - **GDPR (EU)**: Protects patient data processed by health-tech companies operating in the EU.
    - **European Health Data Space (EU)**: Proposed regulation to standardise health data sharing and protect privacy across EU member states.
- **Partner and Data Standards:**
    - **ISO 27001 (International)**: Sets standards for information security management, which is critical for health-tech companies handling sensitive health data.
- **National Regulations:**
    - **FDA (USA)**: Governs medical devices and digital health products.
    - **NHS & MHRA (UK)**: Regulations for healthcare providers, including tech-based health solutions.
- **Good Manufacturing Practices (GMP)**:
    - International standard for product quality control, required in pharmaceuticals and certain biotech applications
- **EU Clinical Trials Regulation**: Governs clinical trials in the EU, ensuring safety and efficacy in drug development.

- **3.5 Climate tech**

- **Environmental and Sustainability Standards:**
    - **EU Taxonomy Regulation**: Defines sustainable economic activities and requires climate tech companies to disclose their environmental impact

4. VC-specific regulations that may be passed down to startups

Startups working with VCs may need to provide ESG-related KPIs—such as carbon emissions or diversity metrics—as part of increased reporting requirements. This means aligning business strategies with ESG goals and tracking sustainability performance to support VCs in meeting their regulatory obligations.

- **Sustainable Finance Disclosure Regulation (SFDR)**
    - Adopted in March 2021, mandates all investment funds operating (and with LPs) in Europe (independent of domicile) to disclose sustainability-related information for both ESG and non-ESG products