

Physical Repositories & Digital Bioinfrastructures

Active storage



Base storage

First backup



Svalbard

Second backup



Protecting the Future of Genebanks: Data, Security & Responsibility

Genebanks are evolving from **physical repositories** → **digital bio-infrastructures**

Increasing reliance on:

- Genomic databases
- AI-driven phenotyping & breeding models
- Distributed data sharing (FAIR data principles)
- This makes genebanks part of **critical infrastructure ecosystems**

Implication: Cybersecurity is no longer IT – it is **biodiversity protection**

The Threat Landscape for Plant Genetic Resource Genebanks

Key risks:

- Data theft (e.g. genomic datasets, accession metadata)
- Ransomware on seed inventory systems
- Manipulation of genetic or passport data
- Supply chain attacks (lab systems, cloud providers)
- AI model poisoning (future risk)

Emerging concern:

- “Bio-digital convergence” → cyber attacks can impact **food security and sovereignty**

International agreements

- 1992: Convention on *Biological Diversity* (CBD) / sovereignty
- 2004: The International Treaty on Plant Genetic Resources for *Food and Agriculture* (ITPGRFA) / MLS & SMTA
- 2014: Nagoya Protocol (Convention on Biological Diversity)



Convention on
Biological Diversity



The International Treaty
ON PLANT GENETIC RESOURCES FOR FOOD AND AGRICULTURE

SUSTAINABLE DEVELOPMENT GOALS



Legal Requirements



- **GDPR** → Protects sensitive data (including genetic data)
- **NIS2** → Requires cybersecurity for NordGen operations
- **Cyber Resilience Act** → Secures digital systems and devices
- **Data Act & Governance** → Enables safe data sharing
- **EU AI Act** (Analysis & ML) → Data integrity, transparency and traceability
- **Cyber Security Act in Sweden** → Swedish Law regarding cybersecurity and NIS2

NIS2 Directive (Core Framework)

Establishes EU-wide cybersecurity baseline for **critical sectors**

- Requires:
 - Risk management measures
 - Incident reporting (often within 24h)
 - Governance accountability at board level

Key message for genebanks:

Likely classified as:

- Research infrastructure, or
- Critical food/agriculture support system
- Management liability is explicit
- Significant penalties for non-compliance



CER Directive (Critical Entity Resilience)

Complements NIS2:

- NIS2 → cyber risks
- CER → **physical + operational resilience**

Implication for genebanks:

Protection must include:

- Seed storage facilities
- Power supply & climate control
- Physical access & insider threats



GDPR (Data Protection)

Applies when:

- Personal data in research datasets (as well as genebank admin)
- Indigenous knowledge / farmer-linked metadata



Cybersecurity relevance:

- Data breaches = legal + reputational risk
- Requires:
 - Data minimisation
 - Encryption & access controls



Cyber Resilience Act (CRA)

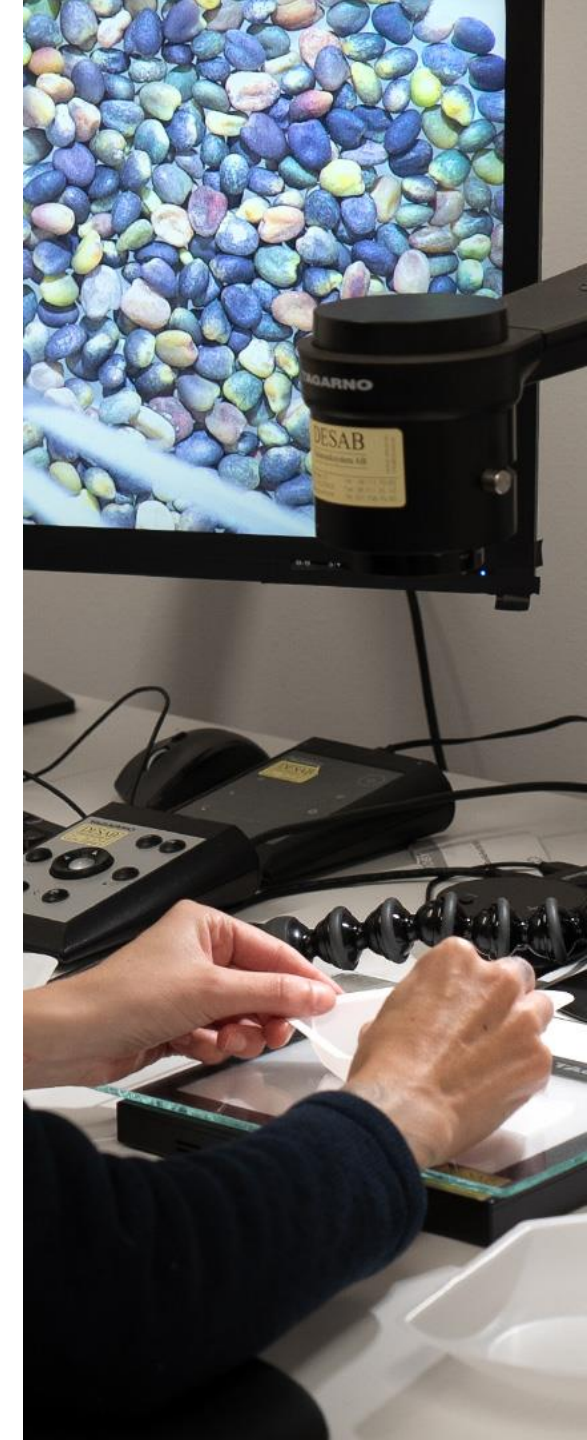
Applies to **all digital products and software** used by genebanks

Requires:

- Secure-by-design systems
- Lifecycle vulnerability management
- Mandatory updates & patching

Implication:

- LIMS systems, IoT sensors, lab equipment → must be compliant
- Procurement becomes a cybersecurity function



EU AI Act

Regulates AI systems with a **risk-based approach**

— High-risk AI must include:

- Security against data/model manipulation
- Transparency and traceability

For genebanks:

AI used for:

- Trait prediction
 - Genomic selection
- must be **auditable and secure**



Swedish Cybersecurity Act (example of national implementation)

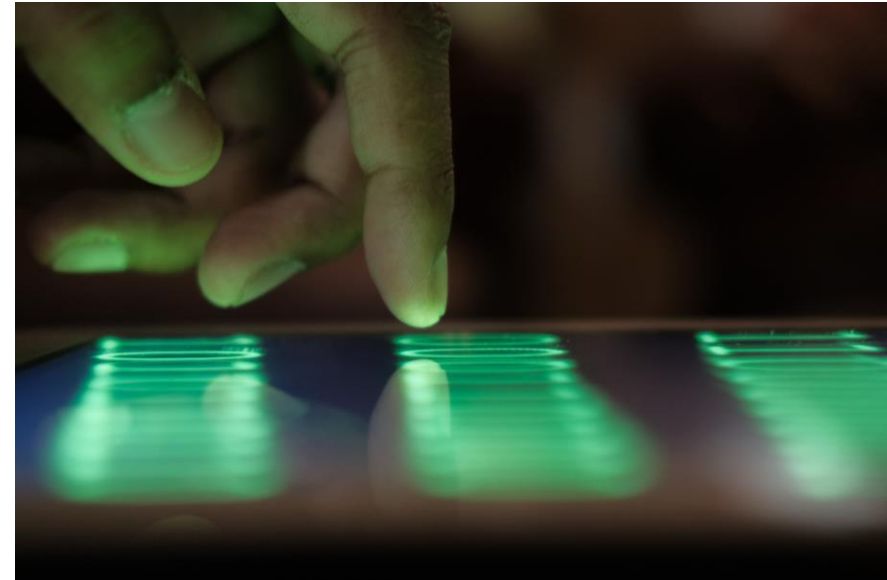
Implements NIS2 from **January 2026**

Introduces:

- Whole-entity responsibility
- Risk-based minimum controls
- Mandatory reporting to authorities

Key takeaway:

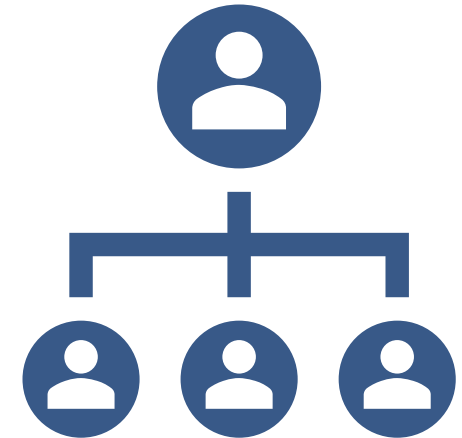
- National laws will **increase enforcement pressure significantly**



Key Cybersecurity Priorities for Genebanks

Governance & Leadership

- Board-level responsibility (NIS2 requirement)
- Appoint:
 - Security lead (incl Incident response person)



Infrastructure Security

Protect:

- Seed storage systems (temperature, humidity control)
- Laboratory systems (LIMS)
- Cloud platforms (move away from US solutions)

Implement:

- Network segmentation
- Backup & recovery (offline backups critical)



AI & Data Integrity Security

Protect against:

- Data poisoning
- Model manipulation

Ensure:

- Traceable datasets
- Reproducible pipelines



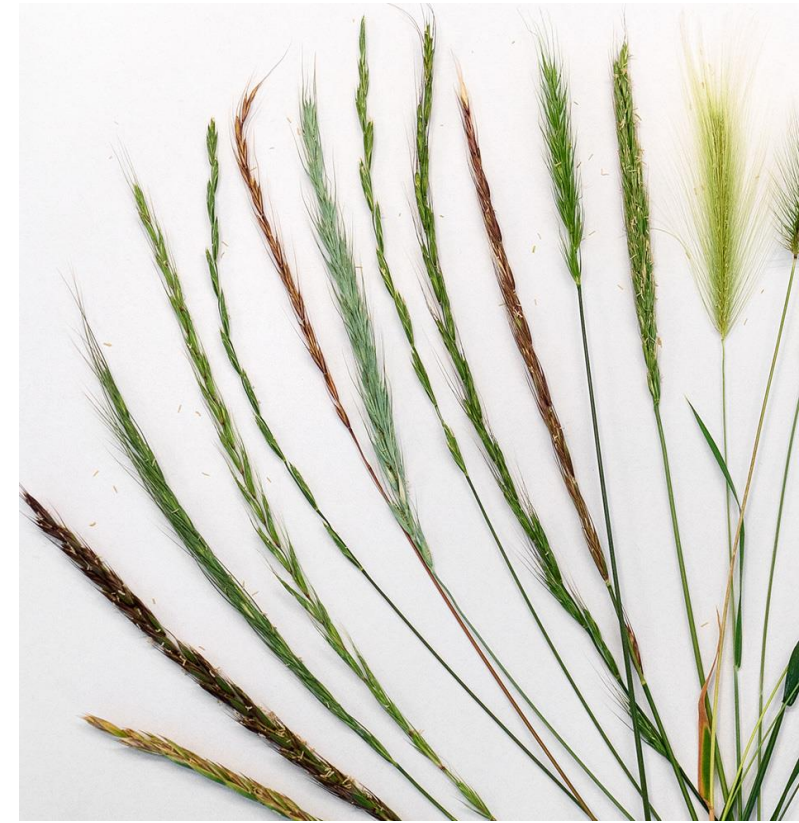
Strategic Risks Unique to Genebanks

Loss of genetic diversity data = **irreversible damage**

Data manipulation could:

- Mislead breeding programs
- Impact global food systems

Increasing geopolitical interest in genetic resources



Traceability Gap

Physical → Digital → Breeding Outcome

- Weak linkage between accessions, genomic data, and final varieties
- No harmonised system for tracking genetic resource utilization
- Increasing gap between physical samples and Digital Sequence Information (DSI)

Unclear ABS Application in Genomics & AI Breeding

Uncertainty around Access & Benefit Sharing for:

- sequence data (DSI)
- trait predictions
- digital breeding models

The lack of a clear link between digital genetic information and benefit-sharing systems

NordGen's approach

- Overall preparedness plan
- Gap Analysis
- Up to date IT Policy
- Access Control (MFA)
- Regular backup of the database (3 copies)
- Proper Monitoring System
- Each Department has different Network(VLAN)
- Regular Vulnerability test
- Security Operation Center (SOC)

Future Implementation Plan

- Real time Incident Response
- Incorporating Modern Threat Intel
- Track all Data from Single Portal (Unified data governance)
- Security Awareness training for everybody
- Strong Supply Chain Management
- Increasing data security
 - Plan to shift EU based solutions

Let's share our efforts & knowledge and learn from each other

- A cyber incident in a genebank is not just an IT problem
 - It is a scientific problem
 - It is a reputational problem
 - And increasingly, it is a geopolitical problem

Thank you!

Lene Krøl Andersen

Director

NordGen

Lene.krol.andersen@nordgen.org

