EU Security Union - 2ND INFOSHARE

NIS-2, CER, CRA: State of affairs and next steps

Cathrin Stover, Alf Moens, Edit Herczog
Rules of engagement

• This session is recorded
• Please mute
• Ask questions in the chat:
  • we will try to answer as many as possible, given time and expertise
• Time permitting we will have a short Q&A at the end of this infoshare
• Ask questions later:
  • Visit the wiki pages
  • Join SIG-ISM
  • Ask your CISO/Security officer/legal counselor
  • Ask your GÉANT partner relations representative
  • Ask the GN5-1 WP8 security team
## Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.00</td>
<td>Welcome and introduction</td>
<td>Cathrin Stover</td>
</tr>
<tr>
<td>13.10</td>
<td>Quick Summary</td>
<td>Alf Moens</td>
</tr>
<tr>
<td>13.15</td>
<td>The EU Security Union, what it is and where are we now?</td>
<td>Edit Herczog</td>
</tr>
<tr>
<td>13.35</td>
<td>Impact of NIS-2 for R&amp;E</td>
<td>Alf Moens</td>
</tr>
<tr>
<td>13.45</td>
<td>What <strong>you</strong> need to do <strong>now</strong></td>
<td>Alf Moens</td>
</tr>
<tr>
<td>13.55</td>
<td>What we will do together</td>
<td></td>
</tr>
<tr>
<td>14.10</td>
<td>Questions and Answers, discussion</td>
<td></td>
</tr>
<tr>
<td>14.25</td>
<td>Conclusions, Next steps and closing</td>
<td></td>
</tr>
</tbody>
</table>
Quick Summary

• **NIS-2 directive** has been published on 15th of December 2022, and will be in action within 21 months from the “entry in force”:

• **4th of October 2024**: (January 4th 2023+ 21 months) latest, but with the Council Recommendation **to do it ASAP**.

• Standards are still ‘negotiated’ via comitology (delegated Act)
  • Cybersecurity Certification scheme

• Obligations are „logical”, no real surprises
New EU Legislation
A number of new EU regulations are due shortly, on security, data governance, data market and more.

NIS-2 Directive
The new security directive will directly impact GÉANT and the NRENs

Directive on the resilience of critical entities (EC/1/CER)

EU Cybersecurity Act (2019)
&
Security Union 2020 – 2025 Strategy (July 2020)
&
Cybersecurity Strategy for the Digital Decade (December 2020)

European Cybersecurity Industrial, Technology and Research Competence Centre
Network of National Coordination Centers

Joint Cyber Unit
EU Cyber Capacity Building Board

Certain research areas identified that require heightened security measures: health, Earth observation and security research
NIS-2 Directive

What is it?
A directive to enforce the implementation of adequate security measures for information systems the society depends upon.

Who is it for?
Organisations in almost all sectors that are vital or important to keep society afloat.

In or out of scope?
This directive is aimed to broaden the scope of the previous one and make it more explicit.

Impact on security
Organisations will have to comply with international security standards and they will have to show compliance.

Supervision and auditing
There will be a national supervising body that will also have the power to enforce compliance. Peer reviewing and external auditing are to be expected.

Research and Education is intentionally included and mentioned, will be MS discretion.
Essential or Important entity

Oversight
- The entity is the sole provider of a service in a Member State
- The entity is critical because of its specific importance at national level or for a particular sector

Government Agency
If you are a government agency you are within scope.

TLD
If you are the registry of a TLD you are within scope

DNS
DNS service providers provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers

Cloud and trust Services
The EU Security Union is complex and overlaps with the EU Digital priorities

Digital Education Action Plan for 2021-2027
The European Education Area by 2025
A new European Research Area for Research and Innovation

The EU Security Union Strategy

European Commission, Factsheet: The EU Union Strategy (IP of December 2020)
Timelines for NIS-2, CER, CRA

Due to the current alarm levels MSs have agreed to frontload enforcement even before the legislation is transposed. Critical infrastructure protection in digital sector modelled on 5G cybersecurity Toolbox.

- **NIS2**
  - European legislation
  - Published in the OJ 15th of December 2022
  - Transposition via National Parliament Maximum 21 months

- **CER**
  - European legislation

- **CRA**
  - European legislation
  - Enforcement

- **Enforcement**
  - 2020
  - 2022
  - 2023
  - 2024
  - 2025
  - 2026
The Main Difference between NIS-2 CER and CRA

CER /NIS2  
Entity Driven  
Extraterritorial like GDPR

CRA  
Product driven underpinned by  
General Product Safety Regulation  
Machinery Directive

Cybersecurity Act Certification

Certification via Delegated Acts (ENISA)
What to negotiate during transposition: NREN-s and GÉANT

- **Scope**
  - Domain
    - Public Administration
    - Education
  - Qualification of Specific entities
    - Essential: Digital infrastructures are here
    - Important

- **National Cyber Security Strategy (examples)**
  - Governance Framework
  - Public Procurement Specification
  - Policy on the open Internet and Submarine cables
  - Policy on support to R&D Communities

**Suggestion**

1. The opportunity to opt out is impossible
2. To be an important entity is not feasible (as definition of RI is very specific)
3. Among Essential types Digital Infrastructure is the best. (avoid CER additional requirements)

**Conclusion**

Member States will differ, coordination among NREN/s is recommended

**Objective**

Minimize the burden and fragmentation
What is the NIS-2 directive about?

Obligations for Member States

Implementation guidance, governance and control for MS

Obligations to report security incidents

International Collaboration

Obligations for Essential and Important entities

Union level coordinated security risk assessments of critical supply chains

Cybersecurity information sharing

Vulnerability disclosure & European Vuln. database

Use of European cybersecurity certification schemes

Obligations to report security incidents

Union level coordinated security risk assessments of critical supply chains
Competent authorities and single points of contact

- Competent authority will:
  - Decide upon who is in scope
  - Take care of registration of entities within scope
  - Have supervising task

- May not be the same supervisor/coordinator as for NIS-1 (mainly telco!)

- Cooperation at international level (for Member States):
  - Cooperation Group
  - CSIRT network
  - European cyber crisis liaison organisation network (EU-Cyclone)
  - ENISA
Impact of NIS-2 for Research and Education: in scope or out-of-scope

Type of organisation
- Public Administration
- Registrar
- Internet exchange
- ...

Example of negotiations:
- Size* of a tld determines whether registry is in/out scope
- However negotiations between Member States: NL 300.000+, D: 500+

Aim to be a digital infrastructure, either an essential or an important entity. Most NREN’s should not be in scope of CER.

Example of negotiations:
- Scoping decisions are made on a national (Member State) level

“The entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities” (art. 2.2.b)

“The entity is critical because of its specific importance at national ... level for the particular sector …, or for other interdependent sectors” (art.2.2.e)

Essential or important? Same rules apply except the oversight

*Caution
The Size criteria is overruled by Article 2.2 „Regardless of their size…”
Cross border impact

This is especially the case for GÉANT, Nordunet and possibly also for some research infrastructures

- Supervision
- Incidents with cross-border impact
Article 21
Cybersecurity risk-management measures

“based on an all-hazards approach”

a. Policies on risk analysis and information system security;
b. Incident handling;
c. Business continuity, such as backup management and disaster recovery, and crisis management;
d. Supply chain security;
e. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
f. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
g. Basic cyber hygiene practices and training;
h. Cryptography and, where appropriate, encryption;
i. Human resources security, access control policies and asset management;
j. Multi-factor authentication or continuous authentication solutions
Information Security Standards

- ISO 27001 and 27002
- NIST
- Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures
- Measures for TLD registries
- GÉANT Security Baseline
- National standards
Cybersecurity of 5G networks EU Toolbox of risk mitigating measures

- Originally aimed at Telco’s
- Commissioner Vestager (EC)

Table 1 - Risk categories and scenarios
(source: the EU coordinated risk assessment report)

<table>
<thead>
<tr>
<th>I - Risk scenarios related to insufficient security measures</th>
<th>R1 - Misconfiguration of networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>R2 - Lack of access controls</td>
<td></td>
</tr>
<tr>
<td>R3 - Low product quality</td>
<td></td>
</tr>
<tr>
<td>R4 - Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>II - Risk scenarios related to 5G supply chain</th>
<th>R5 - State interference through 5G supply chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>R6 - Exploitation of 5G networks by organised crime or organised crime group targeting end-users</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>III - Risk scenarios related to modus operandi of main threat actors</th>
<th>R7 - Significant disruption of critical infrastructures or services</th>
</tr>
</thead>
<tbody>
<tr>
<td>R8 - Massive failure of networks due to interruption of electricity supply or other support systems</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IV - Risk scenarios related to interdependencies between 5G networks and other critical systems</th>
<th>R9 - Exploitation of IoT (Internet of Things), handsets or smart devices</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>V - Risk scenarios related to end user devices</th>
</tr>
</thead>
</table>

Table 2- Toolbox measures and supporting actions

RISKS

MITIGATING MEASURES

STRATEGIC MEASURES
a) Regulatory powers
b) Third party suppliers
c) Diversification of suppliers
d) Sustainability and diversity of 5G supply and value chain

TECHNICAL MEASURES
a) Network security - baseline measures
b) Network security - 5G specific measures
c) Requirements related to suppliers’ processes and equipment
d) Resilience and continuity

SUPPORTING ACTIONS

enabled, supported or made effective with

enable, assist or improve effectiveness of
Strategic measures

... Technical measures

TM01 Ensuring the application of baseline security requirements (secure network design and architecture);
TM02 Ensuring and evaluating the implementation of security measures in existing 5G standards;
TM03 Ensuring strict access controls;
TM04 Increasing the security of virtualised network functions;
TM05 Ensuring secure 5G network management, operation and monitoring;
TM06 Reinforcing physical security;
TM07 Reinforcing software integrity, update and patch management;
TM08 Raising the security standards in suppliers’ processes through robust procurement conditions;
TM09 Using EU certification for 5G network components, customer equipment and/or suppliers’ processes;
TM10 Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services);
TM11 Reinforcing resilience and continuity plans.

Additional measures

SA01 guidelines and best practices on (network) security;
SA02 testing and auditing capabilities at national and EU level;
SA03 Supporting and shaping 5G standardisation;
SA04 Developing guidance on the implementation of security measures in existing 5G standards;
SA05 Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme;
SA06 Exchanging best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers;
SA07 Improving coordination in incident response and crisis management;
SA08 Conducting audits of interdependencies (between 5G networks and other) critical services;
SA09 Enhancing cooperation, coordination and information sharing mechanisms;
SA10 Ensuring (5G deployment) projects supported with public funding take into account cybersecurity risks.
Good Security Practices

- Risk management
- Basic Security requirements
  - Roles and responsibilities, some policies
  - System hardening
- Strict access control
- Network (and system) management, operation and monitoring
- Patch management
- Robust procurement conditions
- Resilience, continuity and recovery plans

- Incident response capabilities
- Information sharing
What do we already know and have?

• Overview of agencies per member state: *This is a good starting point to get in contact with national authorities. We will work on sharing the latest information*

• GÉANT Security Baseline: *helps you assess your status, easy to use, we can assist*

• Policies, best practices, Risk management policy

• SIG-ISM: security management community

What do we want to know?

• Coordinator per NREN

• Your status:
  • Your NIS-2-status
  • What you need
NIS-2 agencies/Single-point-of-contact per member state

• Link from NIS coordination group plus examples: List of SPOCS & Competent authorities – NIS Directive
Quick Scans / assessments

- Several NRENs perform maturity scans with their constituents
  - SURF, SIKT, JISC, ...
  - Some of these tools can be shared
- Some countries already have ‘standards’
  - UK: cyber essentials

- Quick scan based on 5G networks toolkit
- Quick scan based on GÉANT Security Baseline
What is the minimal set for security for a NREN?
How are you doing compared to others? Let’s benchmark

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Base</td>
</tr>
<tr>
<td>2</td>
<td>Advanced</td>
</tr>
<tr>
<td>3</td>
<td>Expert</td>
</tr>
</tbody>
</table>

**Security Baselining**

- **NO 01: Policy**
  - Management Commitment and Mandate
  - Internal Security Policy
  - Acceptable Use Policy
  - Regulatory and Privacy

- **NO 02: People**
  - Training and Awareness
  - Personnel Management
  - Supplier Management

- **NO 03: Threats**
  - Risk Management
  - Incident Management
  - Business Continuity Management

- **NO 04: Operations**
  - Tools
  - Cryptography
  - Access Management
  - Patch Management
  - Vulnerability Management
Security Baselining

**Baseline**
80% of NRENs
Entry-level security
The majority of NRENs are already compliant

**Advanced**
30% of NRENs
Solid security practices
Some NRENs are already compliant, most implement just individual requirements

**Expert**
10% of NRENs
Sophisticated security programme
Only a few NRENs are compliant
This is a long-term goal to achieve
### Baseline, example, 2.3 supplier management & 3.3 Business Continuity

<table>
<thead>
<tr>
<th>NO2.3</th>
<th>Requirements</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO2.3.1</td>
<td>A supplier security policy is in place and accessible for staff involved in contracting suppliers.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NO2.3.2</td>
<td>All suppliers have contracts stating relevant security aspects.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NO2.3.3</td>
<td>All suppliers are assessed according to their criticality and business impact and listed at a central location.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NO2.3.4</td>
<td>SLAs, SLA reporting, meeting notes and other documents to assess the suppliers' performance on a regular basis are available.</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>NO2.3.5</td>
<td>Changes in the suppliers' services are monitored on a regular basis</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>NO2.3.6</td>
<td>Where appropriate, suppliers' services and products are audited or penetration-tested.</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO2.3.7</td>
<td>Where appropriate, suppliers handling sensitive data have signed an NDA.</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NO3.3</th>
<th>Requirements</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO3.3.1</td>
<td>A BCM process is defined, documented and implemented.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NO3.3.2</td>
<td>A Business Continuity Manager responsible for the BCM process is assigned.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NO3.3.3</td>
<td>A BCP exists, which covers at least disasters produced by power failure, fire and water.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NO3.3.4</td>
<td>A list of managers responsible for handling disasters at any point in time is defined.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NO3.3.5</td>
<td>The BCP covers all NREN-specific disasters from the GÉANT Disaster List.</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>NO3.3.6</td>
<td>The organisation participates yearly in a crisis simulation, such as the GÉANT CLAW workshops.</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO3.3.7</td>
<td>A manager on duty is assigned to be available on call 24/7/365.</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security Baselining (example)

Security maturity

<table>
<thead>
<tr>
<th>Functions</th>
<th>Security Practices</th>
<th>Current</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy and Leadership</td>
<td>Management Commitment and Mandate</td>
<td>1,58</td>
<td>0,33</td>
<td>0,25</td>
<td>1,00</td>
</tr>
<tr>
<td>Policy and Leadership</td>
<td>Internal Security Policy</td>
<td>2,00</td>
<td>1,00</td>
<td>1,00</td>
<td>0,00</td>
</tr>
<tr>
<td>Policy and Leadership</td>
<td>Acceptable Use Policy</td>
<td>2,08</td>
<td>0,83</td>
<td>0,75</td>
<td>0,50</td>
</tr>
<tr>
<td>Policy and Leadership</td>
<td>Regulatory and Privacy</td>
<td>3,00</td>
<td>1,00</td>
<td>1,00</td>
<td>1,00</td>
</tr>
<tr>
<td>People</td>
<td>Training and Awareness</td>
<td>0,92</td>
<td>0,67</td>
<td>0,25</td>
<td>0,00</td>
</tr>
<tr>
<td>People</td>
<td>Personnel Management</td>
<td>1,58</td>
<td>0,83</td>
<td>0,50</td>
<td>0,25</td>
</tr>
<tr>
<td>People</td>
<td>Supplier Management</td>
<td>1,25</td>
<td>0,50</td>
<td>0,50</td>
<td>0,25</td>
</tr>
<tr>
<td>Threats</td>
<td>Risk Management</td>
<td>1,33</td>
<td>0,83</td>
<td>0,25</td>
<td>0,25</td>
</tr>
<tr>
<td>Threats</td>
<td>Incident Management</td>
<td>0,83</td>
<td>0,33</td>
<td>0,50</td>
<td>0,00</td>
</tr>
<tr>
<td>Threats</td>
<td>Business Continuity Management</td>
<td>1,08</td>
<td>0,83</td>
<td>0,25</td>
<td>0,00</td>
</tr>
<tr>
<td>Operations</td>
<td>Tools</td>
<td>1,58</td>
<td>0,83</td>
<td>0,25</td>
<td>0,50</td>
</tr>
<tr>
<td>Operations</td>
<td>Cryptography</td>
<td>2,25</td>
<td>1,00</td>
<td>0,75</td>
<td>0,50</td>
</tr>
<tr>
<td>Operations</td>
<td>Access Management</td>
<td>0,92</td>
<td>0,67</td>
<td>0,25</td>
<td>0,00</td>
</tr>
<tr>
<td>Operations</td>
<td>Patch Management</td>
<td>0,83</td>
<td>0,33</td>
<td>0,00</td>
<td>0,50</td>
</tr>
<tr>
<td>Operations</td>
<td>Vulnerability Management</td>
<td>1,17</td>
<td>0,67</td>
<td>0,25</td>
<td>0,25</td>
</tr>
</tbody>
</table>

Functions | Current Score |
--- | --- |
Policy and Leadership | 2,17 |
People | 1,25 |
Threats | 1,08 |
Operations | 1,35 |
Supervision and Sanctions

- **Essential entities: ex ante**
- **Important entities: ex post**

**Periodic scans, audits, inspections by supervising body or 3rd parties**

- **suspend temporarily a certification**
- **administrative fines**
  - maximum of at least EUR 7M or of a maximum of at least 1,4% of the total worldwide annual turnover
- **request that the relevant bodies, courts or tribunals, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity (essential entities only)**
SECTORS OF HIGH CRITICALITY (Annex I)

- Energy
- Transport
- Banking
- Financial Market Infrastructure
- Health
- Drinking water
- Waste Water
- Digital infrastructure
- ICT Service management
- Public Administration
- Space

Other Critical SECTORS (Annex II)

- Postal and courier services
- Waste management
- Chemical industry and supply chain
- Food supply chain
- Manufacturing (limited)
- Digital providers
  - Online marketplace
  - Search engines
  - Social networking services
- Research organisations
### SECTORS OF HIGH CRITICALITY (Annex I)
- Energy
- Transport
- Banking
- Financial Market Infrastructure
- Health
- Drinking water
- Waste Water
- Digital infrastructure
- ICT Service management
- Public Administration
- Space

### Other Critical SECTORS (Annex II)
- Postal and courier services
- Waste management

### Digital infrastructure

- Internet Exchange Point providers
- DNS service providers, excluding operators of root name servers
- TLD name registries
- Cloud computing service providers
- Data centre service providers
- Content delivery network providers
- Trust service providers
- Providers of public electronic communications networks
- Providers of publicly available electronic communications services

### Research organisations
What CSIRTs can do

NIS 2 Directive: cybersecurity improvement for all

The final text of the revised European Network and Information Security Directive (NIS 2 Directive) has now been published. This doesn't formally apply in the UK, but does have some helpful comments on using data protection law to support network and information security. I've blogged about these previously but, since the final version significantly changes the draft numbering, I thought it was worth posting a revised index to those posts:

CSIRT (international) Information Sharing: Draft Recital 69, which encouraged incident response and information sharing, is now split across Recitals 120 and 121. The former is now even more explicit that “entities should be encouraged and assisted by Member States to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhancing their capabilities to adequately prevent, detect, respond to or recover from incidents or to mitigate their

https://regulatorydevelopments.jiscinvolve.org/wp/2023/01/05/nis-2-directive-cybersecurity-improvement-for-all/
What you need to do NOW!

• Find out what your position is and try to have that confirmed
• Establish contacts in government

• Establish a baseline position
  • Use the GÉANT security baseline or any other checklist to verify your status on the main security subjects
  • Identify weak spots and gaps
What we can do together

• Share information (official documents and references)
  • https://wiki.geant.org/display/SIGISM/NIS-2+Directive

• Quick scans (confidential)
  • Half day quick scan based on GEANT Security Baseline (on basis of availability security officers in WP8)
  • Full day workshop baseline scan Baseline (on basis of availability security officers in WP8)

• Develop and share good practices and guidance
  • Processes and procedures
  • Model policies
  • Roadmaps
  • Limited options for translating good practices
What we can do together, next steps
SIG-ISM in cooperation with GN5-1 WP8

• SIG-ISM: Information Security Management
• Coordination, dissemination and expertise
• Share best practices

• What do we need from you?
  • Share information and best practices
  • ...
  • Assign a coordinator (CISO, Risk manager, Senior manager)

• Visit the wiki pages
  • Join SIG-ISM
  • Ask your CISO/Security officer/legal counselor
  • Ask your GÉANT partner relations representative
  • Ask the GN5-1 WP8 security team
References

- SIG-ISM whitepaper on risk management: https://wiki.geant.org/display/SIGISM/SIG+ISM+white+paper+risk+management
- GÉANT Security Baseline: https://security.geant.org/baseline/
- “Single point of contact” for each Member State: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53682
- Blogpost Andrew Cormack: https://regulatorydevelopments.jiscinvolve.org/wp/2023/01/05/nis-2-directive-cybersecurity-improvement-for-all/
Any questions?

www.geant.org

© GÉANT Association

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).