

2024-1



**How Do EU Do?**

**유럽은 어떻게?**

# 유럽 연구보안 정책



**[발행일]** 2024.08.05.

**[발행처]** 한-EU 연구협력센터  
Rue de la science 14A  
1040 브뤼셀, 벨기에  
<http://www.k-erc.eu>  
+32 (0)2 880 39 06

**[발행인]** 조우현 센터장

**[담당자]** 임지윤 연구원

본 자료는 한-EU 연구협력센터(KERC)가 발행한 보고서로 상업적 혹은 정치적 목적의 이용을 제외하고 누구나 자유롭게 열람 인용 재가공 할 수 있습니다.

How Do EU Do?

유럽은 어떻게?

# 1 연구보안 개념



## ■ 연구보안 개요

### ○ EU에서 바라보는 연구보안

- EU의 연구보안은 다음과 관련된 위험을 예상하고 관리하는 것을 의미<sup>1)</sup>

1. EU와 회원국의 안보에 영향을 미칠 수 있는 중요한 지식과 기술의 바람직하지 않은 이전 (제3국에서 군사 또는 정보 목적으로 이전되는 경우 등)
2. 제3국에서 연구를 도구화하여 학생과 연구원 사이에 허위정보를 만들거나 자체 검열을 조장하여 EU의 학문적 자유와 연구 진실성(integrity)을 침해하는 등 연구에 악의적인 영향을 미치는 경우
3. 지식과 기술을 활용하여 EU의 가치와 기본적 권리를 억압, 침해, 훼손하는 등 윤리 또는 진실성을 위반하는 경우

1) [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C\\_202403510](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510)

## ○ 연구보안의 필요성

- 국제적 긴장이 고조됨에 따라 EU 연구원들은 국제협력 속 연구보안 위험에 점점 더 많이 노출되고 있으며, 이러한 위험으로 인해 유럽의 연구혁신이 영향을 받을 뿐만 아니라, 안보에 영향을 미치거나 윤리적 규범을 침해하는 방식으로 오용될 수 있음
- 또한, EU의 경쟁국들은 정치적, 경제적, 군사적 우위를 차지하는 데 중요한 지식과 기술 역량을 강화하거나 민간-군사 융합 전략을 적극적으로 추진하고 있으며, 외교, 군사, 경제, 기술 등의 여러 분야를 혼합한 복합위협(Hybrid threats)이 증가
- 이러한 복합위협은 학문적 자유와 연구의 진실성에도 영향을 주며, 제3국으로의 지식과 기술 이전의 위험을 동반할 수 있음
- 이에 따라 유럽 이사회는 복합위협을 구조적으로 평가하고 정책입안자의 상황 인식을 강화하는 것이 중요하며, 국제협력을 개방적이고 안전하게 유지하는 보호 조치가 필요할 것으로 봄



## ○ 경제안보 핵심기술 분야

- EU 집행위원회는 권고안을 통해 10개 EU 경제안보 핵심기술 분야\*를 명시, 그중 4개(첨단반도체, 인공지능, 양자, 생명공학)의 기술 보안 및 기술 유출에 가장 민감한 분야에 우선적으로 위험 평가가 도입됨<sup>2)</sup>

\* 첨단반도체, 인공지능, 양자, 생명공학, 연결성, 첨단 감지 및 센서, 우주, 에너지, 로봇공학 및 자율시스템, 첨단소재

## ○ 위험 평가(Risk appraisal)

- 위험 평가는 국제 연구혁신 협력 파트너십이나 프로젝트에서 발생할 수 있는 여러 위험을 고려하는 것을 의미하며, 이러한 위험을 사전에 판단하여 책임감 있게 관리하는 것을 목적으로 함



2) [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L\\_202302113](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302113)

3) [https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec\\_rtd\\_building-blocks-risk-appraisal.pdf](https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_building-blocks-risk-appraisal.pdf)

- 집행위원회가 제시하는 핵심 평가 요소는 다음과 같음<sup>3)</sup>

구분	핵심 평가 요소	세부 평가 요소
1	기관의 위험 수준	<ul style="list-style-type: none"> <li>• 해당 기관의 강점 및 약점</li> <li>• 연구 분야내 해당 기관의 입지</li> <li>• 기관의 재정적 의존 여부</li> </ul>
2	국제 협력 연구 분야	<ul style="list-style-type: none"> <li>• 보안, 윤리, 인권 측면에서 민감한 연구 분야 및 연구 방법, 인프라와의 관련 여부</li> <li>• 이중용도 기술 관련 여부</li> <li>• 핵심기반기술(Key Enabling Technologies) 관련 여부</li> </ul>
3	국제 파트너가 속한 제3국의 위험 수준	<ul style="list-style-type: none"> <li>• 고위험군인 제3국 프로젝트 포함 여부</li> <li>• 파트너 국가의 연구혁신 제재 유무</li> <li>• 연구 분야의 제3국 관련도, 정부의 해당 분야 세계 선두 정책 유무</li> </ul>
4	국제 파트너 기관의 위험 수준	<ul style="list-style-type: none"> <li>• 보유하고 있는 협력 기관의 정보</li> <li>• 파트너 기관의 정부나 군과의 연계 여부</li> <li>• 파트너 기관의 거버넌스 구조</li> <li>• 파트너 기관의 보안 관련 사건 연루 여부</li> <li>• 관련 연구원과 직원의 배경 및 소속</li> <li>• 파트너 기관의 연구 결과 사용 목적, 협력에 대한 양측의 관심도</li> </ul>

How Do EU Do?

유럽은 어떻게?

# 2 / EU 연구보안 정책



## ■ 정책 방향

### ○ 오픈 사이언스 원칙

- EU는 국제 연구협력에 있어 “가능한 한 개방적이고, 필요에 따라 폐쇄적(as open as possible, as closed as necessary)”이라는 원칙을 기반으로 하여 EU 자금 지원을 신청하거나 프로젝트를 수행할 때 오픈 사이언스 원칙 준수를 의무화함
- 동 원칙에 따라 연구원은 과학 연구(출판물, 데이터, 소프트웨어 등)와 그 보급에 대한 액세스를 허용해야 하는 한편, 연구 결과와 데이터를 오픈 액세스로 공개하는 것이 연구원의 정당한 이익에 반하는 경우 비공개로 유지할 수 있음

## ■ 주요 정책 추진 내용

### ○ 유럽경제안보전략<sup>4)</sup>

- '23년 채택된 유럽경제안보전략은 EU, 국가 및 기업 차원에서 경제 안보에 대한 위협을 평가하고 관리하기 위한 프레임워크를 제시하여 연구혁신 개방성을 유지하는 동시에 연구보안을 강화하고자 함

4) [https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security\\_en#research-security-in-horizon-europe](https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security_en#research-security-in-horizon-europe)

- 동 전략은 '기술 보안 및 기술 유출과 관련된 위험'을 주요 위험 중 하나로 판단하여, 개방성이 혁신적 경제의 기반이라는 것을 인정함과 동시에 중요한 부문에서 위험을 줄이고 기술적 우위를 증진하는 경제 안보에 대한 포괄적인 접근 방식의 필요성을 인식
- 경제안보전략의 일환으로, '24년 집행위원회는 잠재적 이중용도 기술 R&D 지원 강화 백서와 연구 보안 강화에 대한 이사회 권고를 포함하는 '경제 안보 패키지'를 채택
- 잠재적 이중용도 기술 R&D 지원 강화 백서는 민간 및 국방 목적 모두에 사용될 수 있는 잠재력을 지닌 핵심 기술과 신흥 기술의 경쟁 우위를 유지하는 것을 목표로 유럽경제안보전략의 '촉진 (promote)' 차원에 기여

### ○ EU의 회원국 및 이해관계자를 위한 조치

- EU 수준의 협력과 조정은 유럽연합 전체에서 일관된 접근 방식을 촉진
- EU는 회원국과의 협의하에 외국의 R&I 간섭을 완화하기 위한 툴킷을 개발하였으며, 집행위원회는 또한 유럽단일연구공간(ERA)의 지식 가치화를 위한 지적 자산 관리 실무 강령에 대한 권장사항을 발표
- '24년 1월에는 유럽경제안보전략의 일환으로 연구 보안에 대한 이사회 권고를 제안하여 연구보안 정책의 기반이 되어야 하는 책임 있는 국제화 원칙을 제시

### ○ 연구보안 강화에 대한 이사회 권고

- 동 권고는 유럽경제안보전략 '보호(protect)' 차원에 기여하며 연구보안에 대한 인식 제고를 촉구하고, 국제 파트너와의 연구협력 리스크 평가와 연구보안 강화를 위한 실질적인 지침을 제공
- 이사회 권고는 연구보안에 있어서 EU의 전반적인 시스템 수립을 목표로 하며, 이는 EU는 지식 및 기술이 자유롭게 유통되는 유럽단일연구공간(ERA)을 구축하여 과학기술 기반을 강화하고 연구 활동을 촉진하고자 하는 유럽연합조약(TEU)의 목표와 일치<sup>5)</sup>

5) [https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF)

- 회원국 및 집행위원회에 대한 권고 내용은 다음과 같음

<p><b>회원국 및 집행위</b></p>	<ul style="list-style-type: none"> <li>• 정책 수립 및 시행 시 학문적 자유와 기관의 자율성 및 비차별의 원칙을 준수하는 동시에 개방성과 보안의 균형을 유지할 것</li> </ul>
<p><b>회원국</b></p>	<ul style="list-style-type: none"> <li>• 공통된 국가 정책 및 지원 구조를 수립하고, 연구보안 위험 관리 지원 서비스를 강화하며, 정부와 연구지원기관 및 연구수행기관과의 협력을 강화할 것</li> <li>• (연구지원기관) 연구 프로젝트의 사전 위험을 명확화하고, 위험 평가 및 관리를 수행하며, 보안 조치를 도입하고, 연구보안 전문 지식을 확보할 것</li> <li>• (연구수행기관) 자원을 통합하고, 위험 평가, 연구보안 교육을 수행하며, 연구 수행에 있어 투명성을 보장할 것</li> </ul>
<p><b>집행위</b></p>	<ul style="list-style-type: none"> <li>• 연구보안에 관한 유럽 전문센터 설립 옵션을 포함하여 구조적 지원 방법을 탐색할 것</li> </ul>

### ○ Horizon Europe 규정

- EU 연구혁신 프레임워크 프로그램인 Horizon Europe은 집행위원회의 오픈 사이언스 원칙에 따라 설계됨

- Horizon Europe 전략 계획 2025-2027에서는 연구보안과 관련된 위험을 완화하기 위한 기존 조치를 강조하기 위해 연구보안에 대한 새로운 섹션을 추가하였으며, 연구보안을 보장하는 동시에 개방성의 원칙을 따르는 것의 중요성을 강조함<sup>6)</sup>

6) [https://managenergy.ec.europa.eu/publications/horizon-europe-strategic-plan-2025-2027\\_en](https://managenergy.ec.europa.eu/publications/horizon-europe-strategic-plan-2025-2027_en)



- Horizon Europe 규정에 따른 연구보안 정책은 다음과 같음

<b>20조</b>	<ul style="list-style-type: none"> <li>• 프로그램에 따라 수행되는 모든 조치는 해당 보안 규칙 (특히 무단 공개로부터 기밀 정보를 보호하는 규칙)을 준수해야 하며, 이를 위해 보안 평가를 수행할 수 있음</li> </ul>
<b>22조</b>	<ul style="list-style-type: none"> <li>• EU의 전략적 자산, 이익, 자율성 또는 안보를 보호하기 위해 참여를 제한할 수 있음</li> <li>• EU는 워크프로그램에 추가적인 적격성 기준을 설정할 수 있음 (정책 요구사항이나 조치의 성격 및 목적에 따라 정당화되는 경우)</li> </ul>
<b>40조</b>	<ul style="list-style-type: none"> <li>• 호라이즌 유럽이 지원한 프로젝트의 결과와 관련하여 집행위 또는 기타 자금지원 기관은 제3국(준회원국 제외)에 설립된 법인에 대한 소유권 이전 또는 독점 라이선스 부여에 반대할 수 있음. 이는 양도가 EU 이익에 부합하지 않는 경우 프로젝트 종료 후 최대 4년까지 적용</li> </ul>

### ○ Horizon Europe 보안 평가(Security appraisal) 가이드라인<sup>7)</sup>

- 집행위원회는 Horizon Europe 프로젝트 신청자와 수혜자에게 보안에 민감하거나 기밀 정보를 포함한 프로젝트에 참여하는 경우 따라야 하는 추가적인 절차에 대한 개요를 제공
- 가이드라인은 그랜트 제안서 및 보안 관련 문서 작성 단계에서의 보안 자체 평가 지침을 제공하며, 보안에 민감한 프로젝트 이행 방법을 설명함
- ※ 보안 자체 평가는 EU 보조금 지급 당국(EU granting authorities)이 EU 기밀 정보를 필요로 하는 프로젝트를 판단하기 위해 보조금 협약에 앞서 필수로 수행하는 보안 검토 프로세스의 일부

7) [https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-handle-security-sensitive-projects\\_en.pdf](https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-handle-security-sensitive-projects_en.pdf)

## ■ 기타 정책 및 이니셔티브 추진 내용

### ① 외국인직접투자(FDI) 심사 제도<sup>8)</sup>

- 안보 및 공공질서 유지를 위해 EU에 대한 FDI를 점검하기 위한 규칙 제정

<b>4조</b>	<ul style="list-style-type: none"> <li>주요 인프라, 기술, 이중용도 품목, 주요 자원의 공급, 민감한 정보에 대한 접근, 미디어 등에 대한 영향을 점검해야 하며, 외국인 투자자에 대한 점검을 수행할 수 있음</li> </ul>
<b>8조</b>	<ul style="list-style-type: none"> <li>FDI가 EU 연구혁신 프로그램의 안보 및 공공질서에 영향을 줄 것으로 여겨지는 경우 회원국에 의견을 발표할 수 있음</li> </ul>

- 집행위원회는 모든 EU 회원국에 FDI 심사제도를 구축 및 유지, 운영할 의무를 부과하고, 심사 제도의 핵심요소가 조화되도록 최소 요건을 명시함

- 안보 및 공공질서에 대한 부정적 영향을 판단하는 기준이 확대되었으며, 부정적 영향이 우려될 시 완화 조치를 포함한 조건부 승인 또는 외국인 투자 금지 결정을 내려야 함

### ② 이중용도 품목의 수출, 중개, 기술지원, 운송 및 이전을 통제하기 위한 EU 체제 수립 규정<sup>9)</sup>

- 이중용도 관련 지식과 기술의 불법 확산을 방지하기 위해 제안되었으며, 수출 허가를 받아야 하는 기술의 범위를 확장함

8) <http://data.europa.eu/eli/reg/2019/452/oj>

9) <http://data.europa.eu/eli/reg/2021/821/oj>

## 5조

- 부록에 명시되지 않은 품목 중 내부 억압, 심각한 인권 침해 혹은 국제인도법 위반과 관련된 사이버 감시 품목의 수출에 대한 허가가 필요함

- 이중용도 품목의 수출 통제 분야에 대한 EU 차원의 신속하고 조화된 조치의 필요성을 강조하였으며, 단기 및 중기적 조치를 제안

③ 외국 R&I 간섭 대응 툴킷<sup>10)</sup>

- '22년 집행위원회는 EU의 이익에 반하며, 강압적이고 기만적이며 은밀하고 부패한 외국 R&I 간섭을 완화하고, EU 고등교육기관 및 연구기관이 학문적 자유, 진실성, 기관의 자율성을 포함한 기본적인 가치를 보호하고 직원과 학생, 연구 결과 및 자산을 보호하도록 지원하는 전략과 모범사례를 제시
- 유럽 전역의 R&I에 대한 인식을 강화하고 탄력성을 구축하여 연구보안을 보다 광범위하게 뒷받침하고자 함
- '23년에는 집행위원회의 조정하에 EU 회원국이 참여한 상호학습(MLE)이 진행되어, 관계자를 참여시키며, 외국 간섭 위험을 이해하고, 위험에 대처하는 조치를 논의

④ 유럽단일연구공간(ERA) 내 지식 가치화를 위한 지적 자산 관리 실천 강령<sup>11)</sup>

- 연구 결과와 혁신 기술의 파급력을 높이고 지식 사용을 가속화하는 것을 목표로 모든 R&I 행위자를 대상으로 전략적 지적 자산 관리에 대한 실천 강령을 제시
- 연구원과 혁신가에게 R&I 결과의 전략적 관리, 통제, 보급, 이전 및 활용에 대한 이해를 개선하기 위한 권장사항을 제공
- 전략적 지적 자산 관리 관행을 마련하고, 지적 자산 소유권을 명확히하며 이에 대한 평가 및 모니터링을 수행할 것을 권고

10) <https://data.europa.eu/doi/10.2777/513746>

11) <http://data.europa.eu/eli/reco/2023/499/oj>

How Do EU Do?

유럽은 어떻게?

# 3 EU 및 유럽 주요국 대응 현황



## ■ 유럽 의회, 이사회, 집행위원회 대응 현황

### ○ 유럽 의회

'22.03

- 외국 간섭에 관한 결의안에서 유럽 대학들이 외국에 재정적으로 의존하는 것에 대한 우려를 표했으며, 데이터, 기술, 연구결과가 유출될 위험과 학문적 자유에 영향을 줄 수 있음을 강조

'22.04

- 연구혁신에 대한 글로벌 접근 방식에 관한 결의안을 통해 연구혁신 이해 관계자들에게 학문적 자유에 대한 실질적인 지침을 개발할 것을 집행위에 요청

'23.05

- 안보 및 방위에 관한 결의안에서 민간, 방위, 보안의 연구개발혁신 분열을 극복하려는 집행위의 제안을 채택, 혁신분야에서 이해관계자들과 EU 민간, 방위, 보안 프로그램을 더 잘 연결할 것을 집행위에 요청

'24.01

- 과학 연구의 자유 촉진에 관한 결의안에서 학문적 자유의 균형을 맞추기 위한 의회의 견해를 전달, 안보와 공공 이익을 위한 조치도 연구의 자유를 부당하게 제한하지 않도록 할 것을 촉구

## ○ 유럽 이사회

'22.06

- 연구혁신 국제협력을 위한 원칙과 가치에 관한 결론에서 집행위와 회원국에 외국 간섭에 대처하고 국제 연구혁신 협력에서 위험을 관리하기 위한 조치를 취할 것을 권고

'22.12

- 연구 인프라에 관한 결론에서 연구 인프라 접근에 대한 유럽 현장을 업데이트하기 위한 이니셔티브를 준비할 것을 권고

'23.05

- 경쟁력위원회 회의에서 지식 보안과 책임있는 국제화에 대한 논의를 진행, 연구 윤리에 근거한 국제협력 및 개방성과 보안의 상호 보완성을 보장하는 것의 중요성을 강조

'24.01

- 연구보안 강화에 대한 권고안을 채택, 권고안 제안에 앞서 '23년 12월-'24년 1월 기간 동안 증거 요청이 진행됨

○ 집행위원회 유럽 연구보안 전문센터<sup>12)</sup>

- 집행위원회는 유럽 연구보안 전문센터 설립 옵션을 검토 중이며, 이에 호라이즌 유럽 예산을 동원할 예정이고, 회원국 및 관계자와 논의하여 전문센터의 기능을 탐색할 것
- 집행위원회는 현재 연구보안 관련 문서와 리소스를 모아 온라인 원스톱숍(one-stop shop)을 개발 중이며, '24년 출시 예정
- 유럽 연구보안 전문센터를 집행위원회의 원스톱숍 플랫폼과 연계하여 EU 전역의 실무 커뮤니티를 조직하고 관계자와 구조적 대화를 유지하며 연구보안에 대한 정책 관련 연구를 수행하여 EU 전역의 추세를 분석할 것

12) [https://research-and-innovation.ec.europa.eu/document/download/e82a2fd9-ac12-488a-a948-87639eef10d4\\_en?filename=ec\\_rtd\\_council-recommendation-research-security.pdf](https://research-and-innovation.ec.europa.eu/document/download/e82a2fd9-ac12-488a-a948-87639eef10d4_en?filename=ec_rtd_council-recommendation-research-security.pdf)

○ 집행위원회 다자간 대화(MLD)<sup>13)</sup>

- 국제 연구의 원칙과 가치에 대한 집행위원회의 다자간 대화의 일환으로 연구보안에 대한 워크숍이 진행됨
- EU 회원국과 OECD, UNESCO 등 국제기구 및 여러 유럽 관계자가 모여 ▲연구보안의 개념, ▲국가 정부 및 국가 자금 지원 기관의 연구보안 정책 및 조치 적용, ▲위험 관리에 관한 연구 기관의 역할에 대한 논의를 진행함
- 논의를 통해 효과적인 연구보안에는 개방성과 위험 관리의 균형을 이루는 사례별 접근 방식 및 강력한 국제협력과 연구원에 대한 교육이 필요하며, 연구 진실성 문제를 해결하기 위해 표준을 조화시키고 학문적 자유를 육성해야 함을 강조



13) [https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/europe-world/international-cooperation/multilateral-dialogue-principles-and-values\\_en](https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/europe-world/international-cooperation/multilateral-dialogue-principles-and-values_en)

## ■ 유럽 주요국의 연구보안 정책<sup>14)</sup>

○ '22년 경제협력개발기구(OECD)는 글로벌 연구 생태계의 연구 진실성과 보안에 대한 보고서를 통해 개방성 및 학문의 자유를 보호하고 국제 연구 협력을 촉진하는 동시에 국가와 경제 안보를 보호하기 위한 다양한 정책 이니셔티브와 조치를 설명함<sup>15)</sup>

- 동 보고서는 연구의 국제화로 인해 발생하는 보안 위험에 대해 국가 당국이나 비국가 집단이 연구 활동을 왜곡하거나 연구 결과를 부당하게 이용하는 활동으로 정의
- OECD 13개국의 이니셔티브를 분석한 동 보고서는 연구 보안을 위한 다양한 조치(입법 프레임 워크, 인식 제고 및 역량 강화 활동 등)를 채택해야 하며 국가 및 다자간 협력이 필요하다고 주장
- 또한, 연구 보안에 대한 책임은 국가 중앙정부, 자금지원기관, 연구기관, 대학 및 정부 간 조직 등 모두에게 있음을 강조

○ 연구보안 강화에 관한 이사회의 권고가 채택됨으로써, EU 회원국들은 연구보안에 대해 공동으로 노력하기로 약속<sup>16)</sup>

- 회원국들은 연구계를 위한 일관된 조치와 지원 구조를 개발하고, 그랜트 지원서에 연구보안 질문을 도입하고, 연구 수행 기관이 연구보안 위험 관리 시스템을 도입하도록 장려할 것에 합의
- 집행위원회는 유럽단일연구공간(ERA) 구조를 활용하여 권고안을 후속 조치할 것이라 밝힘

○ 각국의 이니셔티브는 입법 및 비입법 이니셔티브를 포괄하며, 연구 보안과 창의성 사이의 균형을 맞추는 것을 목표로 함

14) [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760387/EPRS\\_BRI\(2024\)760387\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760387/EPRS_BRI(2024)760387_EN.pdf)

15) <https://doi.org/10.1787/1c416f43-en>

16) [https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/eu-member-states-adopt-recommendations-enhance-research-security-2024-05-23\\_en](https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/eu-member-states-adopt-recommendations-enhance-research-security-2024-05-23_en)

○ 독일

- 독일 학술교류처(DAAD)는 `18년 독일 과학인문학위원회의 권고안을 기반으로 국제학술협력역량 센터(KiWi)를 설립하여 연구보안 및 연구 진실성에 관하여 연구원과 학술기관에 국제 협력 활동 가이드를 제공하고, 고등교육기관이 이를 협력 지침으로 채택하도록 함<sup>17)</sup>
- DAAD는 연구원들이 선도적인 과학 강대국이 된 경쟁국과의 연구협력에 있어 발생 가능한 연구 보안 문제를 해결하기 위해 KiWi를 확장하여 법률 조건뿐만 아니라 위험 및 보안 관리를 포함하는 자문 서비스를 제공할 계획
- 또한, 독일 연방교육연구부(BMBF)는 `24년 3월 성명서를 통해 다음과 같이 연구보안 강화를 위한 8가지 연구보안 원칙을 제시<sup>18)</sup>

차원 (Dimensions)	원칙
I) 기존 수단, 구조, 절차의 효율성과 효과성 증대, 자체 규정 강화 및 전문화	① 과학 커뮤니티 자체 규제 수단 검토·개정
II) 지식 및 인식 강화	② 연구보안 공동 가이드라인 개발
	③ 연구보안 문제에 대한 정보 접근성 강화, 중앙 정보 센터의 필요성 평가
	④ 민감한 기술 식별, 연방정부의 특별 관심사인 연구 분야 정의
	⑤ 정보기관의 정보 수집에 대한 과학 시스템 회복력 개선
III) 민간 및 국방 연구 간 시너지 창출	⑥ 과학 기관 의존성 및 협력 관계 공개
	⑦ 민사 조항에 대한 적절성 평가
	⑧ 민간 및 국방 연구 간 협력 강화

- 독일의 막스플랑크 연구소(Max Planck Society)는 `21년 연구원을 위한 지침을 개발하여 연구원들이 국제 협력을 시작하기 전에, 인권, 학문의 자유, 스파이 행위 등과 관련된 위험을 식별하고 최소화할 것을 권고하였으며, 제3자 자금의 경우 행정 본부의 승인을 먼저 받도록 설정
- 라이프니츠 협회(Leibniz Association)는 소속 기관과 연구원들에게 파트너 국가의 정치적 상황과 연구 파트너의 동기를 평가하도록 요구<sup>19)</sup>

17) [https://www.daad.de/en/the-daad/communication-publications/press/press\\_releases/daad-baut-kiwi-aus\\_2023/](https://www.daad.de/en/the-daad/communication-publications/press/press_releases/daad-baut-kiwi-aus_2023/)

18) [https://www.bmbf.de/SharedDocs/Downloads/de/2024/position-paper-research-security.pdf?\\_\\_blob=publicationFile&v=1](https://www.bmbf.de/SharedDocs/Downloads/de/2024/position-paper-research-security.pdf?__blob=publicationFile&v=1)

19) <https://doi.org/10.1787/23074957>



## ○ 프랑스

- 프랑스 국방·국가안보사무국(SGDSN)은 공공 및 사설 기관(연구실, 기업 등) 내에서 지식과 민감한 기술에 대한 액세스를 보호하고자 국가 과학기술 역량 보호를 위한 정책(PPST)을 마련<sup>20)</sup>
- 이는 기술적, 경제적 경쟁자가 전략적 지식 또는 노하우를 탈취하려는 시도 및 전파 또는 테러에 민감한 지식의 오용을 방지하여 국가의 기본적 이익에 대한 공격을 방지하기 위함
- 특히 제한된 체제 구역(ZRR)\*으로 지정된 보호 구역 내에 저장된 민감한 정보에 관한 물리적, 가상적 액세스를 제어하는 것을 기반으로 하는 법적 및 행정적 보호를 제공
- \* 국가에 대한 이익을 위해 보호되어야 하는 연구 또는 생산 활동이 이루어지는 공간
  - 동 정책은 다음과 같은 법적, 행정적 보호를 제공<sup>21)</sup>

- 민감한 공공 및 민간 과학 인프라를 ‘제한된 체제 구역(ZRR)’으로 지정하는 규제 시스템을 구축하여 해당 인프라에 대한 접근 통제
- 기관의 진실성과 경쟁력에 영향을 미치는 악의적 행위(정보의 부정 사용, 민감한 데이터의 도난, 정보 시스템 침입 등)로부터 법적 보호를 제공
- 기관의 보안 수준 향상을 위한 국가 지원
- 보안 문제 해결을 위한 작업 팀 구성

- 프랑스 국립과학연구소(CNRS)는 다음 네 가지 주요 원칙에 기초하여 동 정책을 이행<sup>22)</sup>

- |                                            |                                                      |
|--------------------------------------------|------------------------------------------------------|
| • 연구원에 대한 신뢰<br>(Trust in Researchers)     | • 연구원에 대한 인식<br>(Awareness of researchers)           |
| • 연구원의 수용<br>(Acceptance from researchers) | • 보호 조치의 실용주의<br>(Pragmatism of protection measures) |

20) <https://www.sgdsn.gouv.fr/>21) <https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation>22) <https://international.cnrs.fr/wp-content/uploads/2024/01/CNRS-Contribution-to-Call-for-Evidence-on-Research-Security-ENG.pdf>

## ○ 영국

- 영국 국가방위보안청(NPSA)은 국제 연구협력 시스템의 무결성을 보장하기 위한 ‘신뢰할 수 있는 연구(Trusted Research)’ 이니셔티브를 통해 민감한 연구 및 지적 재산을 도난, 오용 또는 악용으로부터 안전하게 보호할 수 있도록 지원하고, 학계, 산업계, 고위급 리더, 학회 등을 위한 가이드라인을 제공<sup>23)</sup>
- 영국 연구혁신청(UKRI)도 이와 관련된 워크프로그램을 수립하여 협력 활동을 안전하게 수행할 수 있도록 지침 및 지원을 제공하고, 글로벌 연구혁신 생태계를 운영하는 데 있어 관련된 위험을 최소화하고자 함<sup>24)</sup>
- 영국 대학 대표 기관인 Universities UK(UUK)는 대학이 스스로 직원, 학생을 보호하고 국제화와 관련된 위험을 관리하는 지침을 발표하였으며, 대학의 거버넌스 기구와 경영진을 위한 주요 조치와 사례 연구가 포함됨<sup>25)</sup>
- UUK는 동 지침서에서 ▲개인의 인식과 이해의 변화, ▲기관 시스템, 프로세스, 행동의 변화, ▲분야간 시스템과 프로세스의 변화가 국제적 보안 위험을 완화하고 안전한 국제적 파트너십을 유지하는 데 필수적임을 강조하였으며, 대학 경영진이 보안 위험을 인식하는 문화를 조성함으로써 보안 관련 문제에 대한 기관의 회복력을 개선할 수 있다고 주장
- UUK는 대학이 재정적 위험뿐만 아니라 평판 및 윤리, 보안 위험도 고려할 것을 권고하였으며, 대학이 파트너에 대해 알고, 위험 관련 정보에 입각한 결정을 내리고, 직원의 역할과 책임을 명확화할 것을 제안

23) <https://www.npsa.gov.uk/trusted-research>

24) <https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/>

25) <https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation>



**How Do EU Do?**

**유럽은 어떻게?**

**유럽 연구보안 정책**

