CESAER

The strong and united voice of universities
of science and technology in Europe

Keeping science open?

Current challenges in the day-to-day reality of universities

Annexes

18 October 2023

Annex 1: 'as open as possible, as restricted as necessary' in day-to-day practice

Table 1: Open science and possible restrictions to open science practice

Open Science practice[1]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
Study design and process tracking			
Pre-registration Open process[2]: this refers to openly tracking research processes in an appropriate central repository to support the integrity and reproducibility of research findings.	• IP conditions in relation to foreground and background IP[3]. Foreground IP will be especially relevant in relation to commercially valuable or patentable findings	• IP conditions in relation to foreground and background IP. Foreground IP will be especially relevant in relation to commercially valuable or patentable findings • Trade secrets and non-disclosure agreements, that allow for informal communication of research ideas and designs but when in place, they will restrict early registration and tracking of research processes.	IP law, including: • IP action plan for implementation, • Enforcement of intellectual property rights • Patent protection in the EU • Trademark protection in the EU • Industrial design protection • Trade secrets As example: patent laws often prohibit pre-application public disclosure of findings when

[1] This table outlines various stages of the research cycle and examples of measures are currently restricting or enabling open science. Its format is based on various stages of the research cycle as mentioned in Gownaris et al (2022): (a) study design and tracking; (b) data collection; (c) publication; (d) outreach.

[2] Open processes are not frequently implemented due to lack of awareness amongst researchers and other constraints.

[3] Foreground IP is IP created during the course of a project; background IP is existing IP brought into a project.

Open Science practice[1]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
	• Trade secrets[4] and non-disclosure agreements, that allow for informal communication of research ideas and designs but may restrict early registration and tracking of the research process.		granting for inventions. More examples available under the hyperlink above.
Data collection			

[4] European Commission. 2022. Study on the legal protection of trade secrets in the context of the data economy. (GRO/SME/20/F/206) Final Report. Prepared by Alfred Radauer, Martin Bader, Tanya Aplin, Ute Konopka, Nicola Searle, Reinhard Altenburger, Christine Bachner. IMC|FH Krems University of Applied Sciences, Austria; BMG, Management Advisory Group, St. Gallen, King's College, London.

Open Science practice[1]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
FAIR data	Requirements to ensure data protection for commercial, privacy, security, ethical or other reasons.	Requirements to ensure data protection for commercial, privacy, security, ethical or other reasons.	Regulations that either facilitate or restrict the exchange of data, methods and shared access to (cloud) services and (IT) infrastructure, such as: ● European Strategy for Data (2020) ● Open Research Europe ● PSI Directive 2019/1024 ● General Data Protection Regulation (2018) ● Open Data Directive (2019) ● EU Data Governance Act (2022) ● The proposed EU Data Act
Open-source software (OSS) and code	IP conditions[5] in relation to foreground and background IP, for example when computer code is deemed to be commercially valuable or when open source creates security issues. Some employers have restrictive software policies. Conditions also relate to business models for OSS.	IP conditions in relation to foreground and background IP, for example when computer code is deemed to be commercially valuable or when open source creates security issues. Some universities may have restrictive software policies.	Open source software applications are not necessarily in the public domain, they often come with licences with particular terms and conditions. If so, the Dual-use regulation (2021/821) may apply in exceptional cases..

[5] IP protection on software can include: trade marks, patents, copyrights, design, utility models, database law, confidentiality (trade secrets), complexity of products and services, leveraging other assets, time to market or through internet domain names (EU Intellectual Property Office, 2020).

Open Science practice[1]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
Open-source hardware	While not formally restricted, there are practical challenges that currently restricts the further development of open-source hardware, including concerns related to product liability, safety concerns or certification. IP conditions may be applied.	While not formally restricted, there are practical challenges that currently restrict the further development of open-source hardware, including concerns related to product liability, safety concerns or certification. IP conditions may be applied.	Information security hardware, software and technology (including encryption and cryptanalysis) can be affected by the export regime on dual-use.
Citizen Science	Practical concerns (timing, deliverables, allocation of resources, confidentiality, conditions restricting activism). In some cases conditioned by research integrity policy and/or ethics (e.g. on the participation of citizens as test subjects in health-related research). Concerns related to data quality, data protection and privacy. Volunteer rights and obligations.	Practical concerns (timing, deliverables, allocation of resources, confidentiality, conditions restricting activism). In some cases conditioned by research integrity policy and/or ethics (e.g. on the participation of citizens as test subjects in health-related research). Concerns related to data quality, data protection and privacy. Volunteer rights and obligations.	General Data Protection Regulation (European Commission, 2018) Codes of conduct on research integrity or ethics, such as the European Code of Conduct for Research Integrity
Publication			

Open Science practice[1]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
Open access publications Open peer review	when open access is not supported by international co-authors or their institutions	Lack of support structure for open access publications Lack of resources / funding	Dual-use regulation 2021/821. According to EU recommendation 2021/1700, restrictions may apply when publications are related to controlled technologies [similar to publications behind a pay-wall].
Outreach			
IP sharing and permissive licensing, data altruism, reuse of public data	IP concerns around sharing commercially valuable findings may restrict (early) publication.	IP concerns around sharing commercially valuable findings may restrict (early) publication.	Data sovereignty may be applied in relation to data storage on (non-) European collaborative platforms and data use and benefits.
Open educational resources	Partners may restrict open educational resources by choice of: ● Content provided ● IP protection ● Certification.	Universities may restrict open educational resources by choice of: ● Content provided ● IP protection ● certification.	Open educational resources may be restricted in terms of: ● IP law / regulation ● Accreditation norms. ● Export control

Open Science practice[1]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
Participation in seminars and conferences	Specific conditions for participation, e.g. only open to members of networks, alliances, on invitation only.	Specific conditions for participation, e.g. only open to members of networks, alliances, on invitation only.	Generally not restricted by authorities, funding agencies or the EU

Table 2: Openness-of-science and possible restrictions to 'openness-of-science'

Openness for:[6]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
Human Resources			
HR / recruitment	Conditions, such as: ● Qualifications ● Language proficiency ● Attendance requirements (home/work) ● Security conditions	Pre-employment screening for: ● particular positions, groups or functionalities ● double, honorary or consultant appointments ● visiting scholars, guest researchers, external staff	● International sanctions ● security screening ● visa vetting
Data and management information			

[6] Table 2 outlines key practices that affect the open culture and accessibility of science and technology to other sectors, stakeholders, or nationalities. It includes various '*open-for-science'* practices, seeking to minimise barriers to (inter)national academic and scientific cooperation.The format is based on the management of selected operational processes at universities.

Openness for:[6]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
Access to ● Sensitive data ● Institutional data ● Technical data ● Financial information ● Management Information ● Operational systems ● Project information	a. Contracts and agreements ● Trade secrets ● IP, patents, licences ● Security conditions ● Confidentiality clauses ● Membership conditions b. The use of technical means, such as: internal authorisation protocols, data pools, encryption, compartmentalisation, geo-fencing (location-specific restrictions).	a. HR policy that allows functional access to specified members of staff, such as project security officer(s), data stewards, archiving staff, ICT operators, etc.. b. Data management policy, e.g. with reference to confidentiality, classification of information and data storage; cybersecurity policy c. The use of technical means, such as: internal university authorisation protocols, data pools, encryption, compartmentalisation, geo-fencing (location-specific restrictions).	Supervision requirements and classification instructions for particular: ● Research programs ● Research infrastructure ● International networks ● Research groups Example: the Program Security Instruction (PSI) of Horizon Europe or the Algemene Beveiligingseisen Defensieopdrachten (ABDO) in the Netherlands
Mobility management			
Student and staff mobility	Conditions, such as: ● Qualifications ● Language proficiency ● Attendance requirements ● Security conditions ● Resources / funding requirements	May be restricted, based on: ● Merit (quality-based, language proficiency conditions) ● Caps on number of (international) students ● Financial conditions (e.g. payment of full fee in advance to avoid fake applications) ● Available resources ● Internal security screening	● International sanctions on technical assistance in particular domains may affect eligibility for students and PhD students ● Security screening and visa vetting for PhD students and student applications (e.g. ATAS scheme UK) ● Conditions outlined by mobility programs, such as the Erasmus+ program

Openness for:[6]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
International collaboration			
Collaboration with partners and in networks/consortia	Partners' policy on, and experiences with, collaboration with universities	Internationalisation policy with criteria for the eligibility or selection of partners. Risk assessments, classification, due diligence procedure or ethics procedure, to decide upon the acceptance or selection of research partners.	• International sanctions on persons, entities, countries • Export control regimes with controlled technology • Security conditions for research under specific grants (e.g. EDF grants) • Permission by national authorities may be required for sensitive collaborations

Openness for:[6]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
Data management and IP management in collaboration with partners and in networks/consortia	• IP conditions, licences, trade secrets • Non-disclosure agreements (NDAs) • Conditions for access to data-sets • Conditions with regard to timing: sharing data in pre-competitive space; • Embargoes on publication or re-use	Agreements on : • Foreground and background IP • Data protection • Re-use policy • Retention location and access privileges	Guidelines, such as: • EOSC-Pillar guidelines for legal compliance of researchers • Horizon (EU) or Erasmus+ • European Defense Fund
(Campus) Facility Management			
Access to buildings and labs, facilities, infrastructure	protocols, registers, authorisations, entry passes.	• University authorisation for access to particular buildings and labs • Risk inventories & evaluations (RIE) • Regular vulnerability or (IT) security analyses to inform access policy	Screening by national authorities may be required for access to particular buildings and labs
IT management			
Use of digital infrastructure, cloud services, platforms, IT services	Policy on procurement, use and location of: • digital infrastructure • cloud services • platforms • data services • IT services	Policy on procurement, use and location of: • digital infrastructure • cloud services • platforms • data services • IT services	• Digital Services Act • Artificial Intelligence Act • Open Data Directive (2019) • Data Governance Act (2022) • Data Act

Openness for:[6]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
	Funding / user cost / pricing models	Funding / user cost / pricing models	
Open to receive resources (e.g. materials, prototypes, equipment, lab facilities, access to testing facilities)	Restrictions to invite other investors, restrictions to the handling / testing of prototypes, resources provided by benefactors	• Investment screening by universities • Due diligence on benefactors • Internal donations policy • Registration of donations and external funding e.g. from high-risk countries • Restrictions on type of funding, e.g. crowd funding	• Foreign investment screening • Consolidated financial sanctions • Measures to avoid money-laundering
Valorisation and commercialisation			
Openness to public needs and requests from outside, e.g. on public health	• Protection of privacy-sensitive data • protection of data with commercial value • IP conditions	• Funding requirements / resourcing to open up research/data in response to public requests / needs, • Data protection / IP conditions	• GDPR

Openness for:[6]	May be restricted by partners of the university through:	May be restricted by university of Science and Technology through:	May be restricted by the authorities, by funding agencies or the EU through:
Procurement, funding, and investments by third parties	• Investment screening in real estate and/or equipment: • UBO assessment, due diligence or risk assessment • Decision-making structure on procurement and investments • Restrictions on the procurement of IT infrastructure, outsourcing and Cloud services • Support to startups and spin-offs	• Investment screening in real estate and/or equipment: • UBO assessment, Due Diligence procedure, or risk assessments • Decision-making structure on procurement and investments • Restrictions on the procurement of IT infrastructure, outsourcing and Cloud services • Support to startups and spin-offs	• International financial sanctions • National and EU regulations, e.g. on the prevention of money laundering and anti-terrorrism • Foreign investment screening regulations