Ministry of Education, Culture and Science

>Return address P.O. Box 16375 2500 BJ The Hague The Netherlands

President of the House of Representatives
P.O. Box 20018
2500 EA The Hague

Higher Education Directorate
Rijnstraat 50
The Hague
P.O. Box 16375
2500 BJ The Hague
www.rijksoverheid.nl

Reference
26182596

Date 27 November 2020
Subject Knowledge security in higher education and research

World-class higher education and research are not possible without international collaboration and academic talent from all over the world. Dutch knowledge institutions' leading position and good academic reputation depend on the academic freedom that is guaranteed in the Netherlands, and on their openness to the rest of the world.

At the same time, however, we are currently seeing a re-emergence of competition based on power politics between states. When states promote their own interests, this may affect the interests of other states. Acquiring advanced knowledge is a strategic objective for a range of state actors, for economic or military reasons for example. This kind of (advanced) knowledge is also available in the Netherlands. When state actors actively attempt to acquire this knowledge our interests may be harmed. Though not entirely new, these developments do mean that we must now expeditiously review our existing policy and the way it is implemented.

In this letter the government presents a package of measures designed to better safeguard knowledge security in higher education and (applied) research. Their goal is to ensure that international collaboration takes place safely, taking into account both the opportunities and the risks it entails.

Knowledge security means first and foremost preventing undesirable transfer of (sensitive) knowledge and technology, with negative implications for our national security and ability to innovate. It also means preventing covert influence on higher education and research by state actors, which can lead among other things to self-censorship, thus impairing academic freedom. Finally, knowledge security also concerns ethical issues that arise when collaborating with individuals and institutions from countries that do not respect fundamental rights.

The proposed measures are designed to enhance stakeholder awareness of knowledge security and ensure that institutions more sharply define their security policies. The government is also working on an screening mechanism to counter undesirable knowledge and technology transfer in fields with a heightened risk of national security breaches. The measures are aimed at universities, universities of applied science and research institutes, including the applied research institutions.

This letter first defines its context and scope, before turning to developments in the threat analysis. The guiding principles that determine the policy response are then described, after which, in section 4, the policy measures being prepared by the government are set out. The letter ends with a number of closing remarks.

1. Context and scope of this letter

As announced in the policy response to the Rathenau Institute's report '*Kennis in het Vizier',*[1] the government has launched a process to explore to what extent additional measures are needed to mitigate the risk of undesirable knowledge and technology transfer to third countries through (academic) education and research. This letter informs parliament first of all about progress achieved in this process. The answer to the question of whether additional measures are needed is a resounding 'yes'.

Parliament was previously informed of the government-wide integrated approach to state-actor threats, in a letter which discussed matters such as investment screening, export controls, cybersecurity and economic espionage.[2] The present letter examines the knowledge sector, focusing on sector-specific characteristics and threats, while bearing in mind the broader context.

In line with the 2019 National Security Strategy,[3] the concept of national security is used as an umbrella term encompassing several security interests, including economic security. Preventing loss of advanced knowledge and the emergence of strategic dependencies on other state actors enhances our economic security, and thus our national security as a whole.

It is important to underline the fact that the government has deliberately opted for a country-neutral approach. It is intended to be a generic approach applicable to any state actor that poses a threat. Nevertheless, information emerging from country-specific research will be considered in the definition and shaping of policy measures.[4]

2. Developments in the threat analysis

Changes on the global stage are causing economics, geopolitics and security to become ever more closely interwoven. There has been a revival of competition based on power politics between states, leading to shifts on the geopolitical playing field.

State actors or third parties deployed by a state actor (proxies) regularly promote their interests in an assertive and sometimes aggressive manner, abiding only by their own rules. The interests of other countries, such as the Netherlands, are disregarded in the process, either intentionally or unintentionally. Sometimes they are deliberately harmed. The damage caused can become manifest in the short as well as the long term.

We know that also Dutch knowledge institutions are targeted by state actors. Some actors are for example interested in acquiring our technological and

[1] Letter from the Ministry of Economic Affairs and Climate Policy. 'Beleidsreactie op het Rathenau Instituut rapport "Kennis in het vizier"' (Policy response to the Rathenau Institute report 'Focus on Knowledge'), 20 December 2019.
[2] Letter from the Ministry of Justice and Security, 'Tegengaan statelijke dreigingen' ('Countering State-actor Threats'), 18 April 2019.
[3] National Security Strategy, 7 June 2019.
[4] The Ministry of Education, Culture and Science commissioned the Clingendael Institute and the Netherlands Enterprise Agency (RVO) to perform a study. The Clingendael report on China's influence on education in the Netherlands (*'China's invloed op onderwijs in Nederland: een verkenning'*), was submitted to parliament on 3 July 2020. RVO's report on academic collaboration between Dutch and Chinese knowledge institutions ('*Verkenning wetenschappelijke samenwerking Nederlandse en Chinese kennisinstellingen*') will be submitted shortly, together with a policy response to both reports.

scientific knowledge to support their own economy, or knowledge that can be used for weapons programmes. State actors use a range of open and covert means to acquire the knowledge they desire.

There are numerous international partnerships between academic and knowledge institutions in which legitimate knowledge transfer occurs. Knowledge can however unintentionally leak if the agreed parameters are not defined clearly enough, or if research findings are stolen. State actors can have an interest in using researchers and students to obtain access to knowledge. Some state actors deliberately place students or researchers in certain positions in other countries in order to gain this access. Finally, state actors also engage in digital espionage against universities and other knowledge institutions, including phishing attacks to obtain access to systems and files.

The undesirable leakage of sensitive knowledge and technology to other countries means that Dutch innovations recede beyond our borders, undermining our capacity to innovate and our competitiveness. Furthermore, the Netherlands runs the risk that knowledge that is shared may be used against it at a later stage or that international obligations concerning peace and security are not complied with. The knowledge can also potentially be used for purposes incompatible with fundamental norms and values, such as respect for human rights.

3. Guiding principles and assessment framework

The government is as keen as ever on international collaboration in higher education and research, and on attracting international talent. The same goes for its commitment to open science – research that is informed by and connected with society – and on the principle of open access to all publicly funded research, as set out in the letter on science policy of January 2019.[5] The approach presented here does not call into question these commitments.

The principle remains ‘open where possible, protected where necessary’, with proportionality and customisation as the key. It is a matter of ensuring that international collaboration can take place *safely*, striking a healthy balance between opportunities and risks. Measures to guarantee national security must therefore be robust enough to be effective and specific enough to prevent collateral damage, and the cure must not be worse than the disease.

Core scholarly values like academic freedom, scientific integrity, openness, reciprocity, accessibility and institutional autonomy will continue to be the benchmark for our actions. These values are after all an integral part of the interests we seek to protect. As set out in a number of letters on internationalisation and innovation policy, international exchange and knowledge transfer are vital to maintain the position of Dutch higher education and (applied) research.[6]

At the same time, the assessment framework must extend beyond considerations related to higher education and research. Measures to safeguard knowledge security could have implications in other areas. They may, for instance, affect our diplomatic relations and/or our economic interests, including our competitiveness and business climate.

[5] Ministry of Education, Culture and Science letter on science policy, *'Nieuwsgierig en betrokken: de waarde van wetenschap*' (‘Curious and committed – the value of science’), 28 January 2019.
[6] See inter alia the Ministry of Education, Culture and Science letter on internationalisation, *'Internationalisering in evenwicht*' (‘Internationalisation in balance’), 4 June 2018 and the Ministry of Economic Affairs and Climate Policy letter on innovation, *'Naar missiegedreven innovatiebeleid met impact'* (‘Towards a mission-driven, impactful innovation policy’), 13 July 2018.

Naturally, ethical considerations also play a role in international collaboration. There is for example a possibility that in countries where fundamental rights are not respected the knowledge acquired will be used against the population, or that foreign researchers will come under pressure in their home country.

This all has major implications for the responsibility that knowledge institutions in the Netherlands have by virtue of their statutory institutional autonomy. The government realises however that they cannot shoulder this responsibility alone. The government's overarching responsibility for the education and research system means it must work with the sector to determine prospects for action. Knowledge institutions are asking for clarity on the matter and tools to take measures to protect their knowledge and their researchers and students from threats. This requires a government that informs, helps devise solutions, and advises. It also requires a government which sets limits where necessary and ensures they are observed.

In order to be effective, measures need to be defined at EU level wherever possible, and the Netherlands will act in concert with partner countries within and outside the European Union. This reflects the consideration that if the Netherlands acted alone to introduce stringent measures against certain state actors, this might prompt those actors to introduce countermeasures that would mainly or solely affect Dutch business and research. The government is keen to prevent this as much as possible.

4. Policy measures

Against this backdrop, the government has developed a package of measures which, taken together, offer prospects for action for both the knowledge institutions and central government. The measures combine awareness-raising and self-regulation in the knowledge sector (section 4.1) with a binding screening framework for high-risk subject areas (section 4.2).

In this way the government intends to implement the part of the motion by MPs Van der Molen and Wiersma that calls upon it to devise new screening frameworks, clear procedures and unambiguous agreements to ensure that knowledge development with implications for defence and security occurs in a socially responsible manner.[7]

It should be noted that in recent years a great deal has already been set in motion, not least by the institutions themselves. The government already offers institutions possibilities to share knowledge and expertise to help them assess the risks associated with international partnerships. There are of course major differences within the knowledge sector in terms of risk profiles, starting points and awareness. The policy measures must take these differences into account.

Finally, we should point out that several legal frameworks are already in place to help ensure knowledge security. They include sanctions regulations and regulations associated with the Nuclear Energy Act.[8] The export control regime under the EU dual-use regulation (EC 428/2009) also obliges knowledge institutions that develop or produce goods or technology with both civilian and military applications (dual-use technology) to abide by the legislation governing export controls. The export of technology that appears on the lists of controlled goods and technologies in the dual-use regulation requires an export licence.

[7] Motion by MPs Van der Molen and Wiersma concerning new arrangements for knowledge development related to defence and security, 30 June 2020.
[8] Nuclear Facilities and Fissile Material Security Order.

4.1 Awareness and self-regulation

Dutch universities and research institutes must be made structurally more resilient to knowledge security risks. Identifying potential risks is an important first step, but it is not enough in itself. What happens when a potential risk has been identified? How should a researcher, lecturer or board members respond? Do they have adequate response options?

Alertness is not only important at knowledge institutions, but also within central government itself. That is why the government receives briefings from the intelligence and security services, and regularly commissions studies to stay abreast of the methods employed by state actors.

a. Knowledge security dialogue

Central government has launched a knowledge security dialogue consisting of talks at management level with knowledge institutions, to share perceptions of the knowledge security situation at institutions and discuss possible courses of action on the basis of specific cases.

This dialogue, involving several ministries as well as the intelligence and security services, began after the summer with a series of discussions at all universities and research institutes. These discussions will last until the end of January 2021, after which the next phase will begin, focusing notably on universities of applied science.

The knowledge security dialogue's benefits are twofold. On the one hand, it should further raise institutions' awareness of state-actor threats and of the existing instruments available to help them make responsible decisions. On the other hand, the series of talks will give the government valuable insights to be used in further elaborating the measures described in this letter.

The discussion with the Dutch Research Council (NWO) also covered its role and responsibility as a research funding body. In this capacity, it needs to critically assess research partners to which funding is awarded or with which research programmes are managed. This requires a constant focus on the enabling conditions for research, such as academic freedom and open access.

Besides the knowledge security dialogue initiated by the government, there are initiatives and consultations addressing this issue at all levels within the sector. They include the platform on Comprehensive Security in Higher Education (IV-HO), cofinanced by the Ministry of Education, Culture and Science, and a working group on knowledge security at the Association of Universities in the Netherlands (VSNU), with participants from the affiliated universities. NWO, too, regularly organises sessions on knowledge security, and centres of expertise like the LeidenAsiaCentre (LAC) actively help raise awareness with seminars and research reports.

b. Guidelines on knowledge security

Guidelines, checklists and self-evaluation tools can be useful for institutions, helping them to make clear what factors need to be taken into account in international collaboration, and giving them an idea of their own resilience.

Several countries already have such guidelines, including Australia, Germany, the United Kingdom, Sweden and Canada.[9] Also at EU level a document is being developed that could serve as a basis for guidelines at national or institution level.

[9] Australia: 'Guidelines to counter foreign interference in the Australian university sector'; Germany: 'Leitlinien und Standards für internationale Hochschulkooperationen' and 'Leitfragen zur Hochschulkooperationen mit der Volksrepublik China'; United Kingdom: 'Managing risks in internationalisation: Security related issues'; Sweden:

In the Netherlands, the Hague Centre for Strategic Studies (HCSS) and the LeidenAsiaCentre (LAC) have published a joint checklist specifically for collaboration with Chinese universities and research institutions.[10] Previously, in 2014, the Royal Netherlands Academy of Arts and Sciences (KNAW) published a booklet on the challenges and dilemmas associated with international academic collaboration.[11] Also at the level of institutions codes and guidance documents are circulating that refer directly or indirectly to knowledge security.

In light of the experiences of other countries, and considering what is already available in the Netherlands, the Ministry of Education, Culture and Science plans to develop knowledge security guidelines in consultation with the knowledge sector. Its goal is to produce a useful and practicable document that can be used by anyone working at a knowledge institution who is involved in international collaboration. This includes board members, security coordinators, professors and researchers.

The document will need to be country-neutral and tailored to the Dutch situation, taking account of the Dutch system and the mutual relationships within it. It will be based on fundamental principles like institutional autonomy and academic freedom. The aim is to issue the guidelines in the second quarter of 2021.

c. Administrative agreement on knowledge security

Security policy must be more explicitly embedded at the institutions, and the roles and responsibilities of all involved must be made clear. It will not be enough simply to make guidelines available and leave it at that. Institutions will have to assess their internal security policy and, where necessary, review it and tighten up its implementation. In line with institutional autonomy, it is primarily up to the institutions themselves to put this into practice, through self-regulation.[12]

Along with the sector organisations, universities and research institutes, the Ministries of Education, Culture & Science and of Economic Affairs & Climate Policy are therefore working on an administrative agreement,. Its aim is to organise and secure commitment and to work on a common vision of knowledge security. The agreement may cover matters that apply to all subject areas as well as measures that apply specifically to subject areas that are at greater risk of undesirable transfer of knowledge and technology. It will also have to take account of the specific characteristics and starting points of the different parts of the knowledge sector (universities, universities of applied science, research institutes and applied research institutions).

Several matters require particular attention, such as the need for a complete and up-to-date overview at institution level of PhD students associated with the institution and of partnership agreements with foreign knowledge institutions and companies. It is after all in the institution's own interests to have a complete and recent picture so that it can make timely changes if this is called for. The role and position of ethics committees at the institutions is also a matter requiring attention.

The administrative agreement will launch a process designed to consolidate the focus on the issue, obtain a better idea of what is happening in the Netherlands in

'Responsible internationalisation: Guidelines for reflection on international academic collaboration' and Canada: 'Safeguarding your research'

[10] HCSS, 'Checklist for Collaboration with Chinese Universities and Other Research Institutions'.

[11] KNAW, 'International Scientific Cooperation: Challenges and Predicaments', 2014.

[12] Building on existing agreements, including the declaration of intent on a comprehensive security policy in higher education (*integraal veiligheidsbeleid in het hoger onderwijs*), 6 June 2018.

terms of knowledge security, and encourage organisations to learn from each other.

Reference

Potential risks, whether associated with undesirable knowledge transfer, interference and self-censorship or ethical issues, must be properly and continually mapped out by knowledge institutions, so that they can respond quickly and adequately. This requires an internal organisation suited to raising the alarm promptly and at the right level.

The government will consider the effectiveness of this form of self-regulation by means of an administrative agreement when defining the screening framework for undesirable knowledge and technology transfer (see section 4.2).

The aim is to have the administrative agreement in place by the second half of 2021. Institutions need not, of course, wait for the agreements to be officially adopted before taking the necessary measures. They may proceed with this immediately. In practice, various promising examples already exist.

d. Knowledge security centre for expertise and advice

Knowledge institutions are responsible for their own activities, initiatives and partnerships with other countries. These include partnership agreements (MoUs) with foreign partner institutions, public-private partnerships and participation with foreign partners in labs in the Netherlands and abroad, as well as the recruitment of foreign researchers and students, staff exchanges, and PhD students funded by their country of origin.

Institutions have indicated that they take this responsibility seriously, and therefore make every effort to make sound decisions after thorough consideration. However, they also say that they do not always have all the information and expertise they need to obtain the full picture.

Although knowledge institutions can already obtain advice and information from appropriate government bodies, there is a need for a central point to turn to with their questions, and for advice to assist their decision-making.

For example, it may be that a researcher deems the risk of a partnership to be limited from the standpoint of their own discipline, but that government has indications that there are threats to national security. In such situations, it is important that knowledge institutions and government are able to liaise more easily.

To support knowledge institutions in their decision-making as part of their responsibility, the government will launch a centre to provide expertise and advice related to knowledge security.

Such a centre for expertise and advice could act as a liaison, in contact both with the appropriate parts of central government and with the sector organisations. This would guarantee a single point of access for all questions related to knowledge security.

Besides providing general information via briefings, guidelines and events, a centre can also provide quick and easily accessible, tailor-made advice for knowledge institutions. The advice would be non-binding, and would allow institutions to take mitigating measures where necessary. The centre would be intended for anyone involved in international collaboration at knowledge institutions, from board members to individual researchers and lecturers.

For the sake of time and cost efficiency, the possibility of tying in with existing central government initiatives is being explored. If this is found to be possible, the centre's basic services should become operational during the course of 2021.

4.2 Screening framework for high-risk subject areas

a. International sanctions: North Korea and Iran

In March 2019 parliament was informed about intensified monitoring of students and researchers from states of concern.[13] International sanctions banning the transfer of specific knowledge and skills can provide a basis for screening students and researchers. Sanctions are for example in force against North Korea and Iran. In the case of North Korea, the sanctions cover, among other things, the transfer of knowledge that could contribute to North Korea's proliferation-sensitive nuclear activities or the development of means of delivery for nuclear weapons.

As regards North Korea, government decides on the basis of the sanctions regime in force against the country whether an exemption may be granted to give an individual access to specialist knowledge. In the case of Iran, there is a ban on the transfer of goods and technology that could contribute to the development of, among other things, the country's ballistic missile programme, and on the provision of technical assistance in respect of such goods and technologies for use in Iran.

Screening under the EU Regulation on sanctions against Iran focuses on helping universities to prevent these bans from being violated and undesirable knowledge transfer from taking place.[14] Screenings are only carried out in areas of technological research where there is an actual risk of the sanctions being violated. Everyone working in the designated fields of education and research is screened, irrespective of their nationality. The Dutch Supreme Court confirmed in its judgment of 14 December 2012 that no distinction may be made on the basis of nationality.[15]

The experiences and insights gained in this regard provide a useful benchmark for future policy. In response to the motion by MPs Van der Molen and Wiersma, the government does not see any possibility of adding China to a list of countries under intensified monitoring, as there is no basis for assessing students and researchers in connection with China in the absence of applicable UN or EU sanctions.

b. Screening framework for undesirable knowledge and technology transfer

The government's focus is on actively raising security awareness, developing self-evaluation tools like guidelines, and making government expertise quickly and easily available via a centre for expertise and advice. This will create conditions in which knowledge institutions can meet their responsibilities, with respect for their institutional autonomy. Commitment will be secured through an administrative agreement.

However, in some cases self-regulation will not be sufficient, and binding regulations will be unavoidable. Furthermore, the risks associated with undesirable transfer of knowledge and technology are broader than those covered by the above-mentioned sanctions regimes. An screening framework is therefore being developed to curb undesirable knowledge and technology transfer. It will be

[13] Letter from the Ministers of Foreign Affairs, Education, Culture & Science and Justice & Security and the State Secretary for Justice & Security on enhanced supervision of students and researchers from states of concern ('*Verscherpen toezicht op studenten en onderzoekers uit risicolanden*'), 14 March 2019.
[14] Parliamentary Papers 30 821, no. 100.
[15] Judgment of the Supreme Court, ECLI:NL:HR:2012:BX8351, 14 December 2012.

flexible so that it can be scaled up or down according to the nature and severity of the threat.

An inventory of knowledge areas and disciplines requiring protection in the interest of national security is being compiled. Criteria are also being developed that can be used to identify sensitive technologies. This will result in a system that is dynamic and future-proof, and which takes account of new threats and emerging technologies.

The framework will focus on people affiliated with these high-risk subject areas, who have access to the knowledge and technology we seek to protect. These include research staff like (guest) lecturers, researchers, PhD students and (Master's) students, and other people in key positions in the organisation. The experience of countries that already have such a system will be considered when the framework's precise legal form is determined. Some countries link access, directly or indirectly, to visa requirements, for example.

In high-risk subject areas, the government will also examine, in collaboration with knowledge institutions, which elements of partnership agreements with foreign partners (knowledge institutions or companies) are at risk of undesirable knowledge transfer.

Depending on the sensitivity of the knowledge and technology, Dutch knowledge institutions could be obliged to give notification of such agreements once they are concluded (in a mild variant) or submit them for approval before they are concluded (in a strict variant). In highly exceptional cases, where the threat to national security is acute and specific, a (temporary) ban on structured research partnerships with third countries might even be considered. Such a ban would apply until the institution has introduced adequate mitigating measures.

Foreign (research) funding will also be taken into account, in order to prevent excessive (financial) dependence on foreign partners, which could have an impact on academic freedom and integrity.

It makes sense to also apply the same framework to existing partnership agreements and employment contracts which are suspected of presenting a risk.

Once such an screening framework is put in place, it must be properly implemented. Additional legislation will have to be introduced, and general legal principles (such as the principle of non-discrimination) must be respected. Realistically, therefore, a framework will not take effect until 2023 at the earliest. There will also be major financial and technical implications to identify and consider.

The administrative burden resulting from the screening framework will have to be kept to a minimum, for both Dutch knowledge institutions and their foreign partners. In cases where screening is necessary, the length of the procedure must not unnecessarily delay the primary research process, as this could, for instance, cause foreign researchers to lose interest in performing their research in the Netherlands.

At the same time, it must be clear to all parties that the screening framework to prevent undesirable knowledge and technology transfer will be effective only if it is properly and fully implemented by institutions. The government will therefore also consider potential monitoring and enforcement issues.

The effectiveness of self-regulation – under the administrative agreement on knowledge security described above, for example – will be considered when

determining the eventual scope and form of the legally binding screening framework.

5. Efforts in international forums

As indicated above, it is important for the Netherlands to work with partner countries, particularly (though not exclusively) in the context of the EU. Given the highly international character of higher education and research, this is the only effective way of taking robust action against undesirable knowledge and technology transfer. The government will focus first of all on getting the issue of knowledge security on the agenda at expert meetings and, if possible, at political level as well, in the Council of the European Union.

Raising this issue at EU level could initiate a process of peer learning: facilitation of a policy dialogue in which Member States learn from each other and exchange best practices, and in which the European Commission helps by commissioning studies and by providing Member States with non-binding guidance.

One example of this can be seen in the area of research, where guidance is being produced to help Member States and knowledge institutions draw up guidelines to counter interference in education, research and innovation. Work is also under way on guidelines to help knowledge institutions set up a system for dual-use export controls, as legislation in this area also applies to their activities. The Netherlands is actively involved in these initiatives.

Ultimately, raising the issue in the EU could lead to it being incorporated more fully into the terms and conditions of funding under programmes like Horizon Europe and the Erasmus programme. This would allow considerations associated with knowledge security to be taken into account even more extensively in education and research projects funded from EU resources.

There are other pathways, both bilateral and multilateral, that will be taken to enhance knowledge security. They include the Bologna process in higher education and the Council of Europe. As part of the Bologna process, work is now under way safeguarding academic freedom. Multilateral forums like the OECD and UNESCO, where the Netherlands is a champion of open science and open access, could also be used to draw attention to knowledge security.

6. Conclusion

Dutch knowledge institutions face state-actor threats such as the transfer of knowledge and technology that is undesirable from the point of view of national security. Interference and (self-)censorship to which this can give rise undermine academic freedom. Moreover, there are ethical issues associated with collaborating with knowledge institutions and companies from countries where fundamental rights are not respected.

It is expected that these threats are more likely to increase than decrease in the future, so we will have to further enhance our resilience. We must do so in a way that is proportionate and future-proof, and which respects and strengthens the core academic values we wish to protect.

This letter has outlined several policy measures designed to achieve this, measures which, taken together, constitute a comprehensive approach ranging from awareness-raising and information provision to self-regulation enshrined in an administrative agreement. Finally, the government intends to put in place an screening framework to prevent undesirable transfer of knowledge and technology.

It is important to emphasise that, however robust the measures we design, absolute assurances cannot be provided. This is because of the nature of state-actor threats in relation to international collaboration. Situations are often not black-and-white (‘this is allowed’/’this is not allowed’). Something which is allowed may not always be advisable or may even be clearly harmful. Ultimately, therefore, it is a matter of balance, and of carefully weighing up opportunities and risks.

Having said this, the government believes that the measures outlined in this letter will go a long way towards increasing knowledge security in this country. The government will work with knowledge institutions over the coming period to flesh out and implement the measures presented here, and will continue to raise the issue for discussion. Parliament will be informed of progress on this matter in autumn 2021, or earlier if necessary.

the Minister of Education, Culture and Science,

Ingrid van Engelshoven

the Minister of Justice and Security,

Ferd Grapperhaus

the State Secretary for Economic Affairs and Climate Policy,

Mona Keijzer