Safeguarding Dutch Universities Against Big Tech Dominance: Risks and Mitigations

"It is like we have build a firework factory in the middle of a crowded city: if nothing goes wrong there are no problems."*

Jelte Smits
Radboud University Student
Research Internship at SURF

March 28, 2024

Executive summary

Dutch universities have been increasingly **reliant on big tech products** after Covid-19. Despite its ease of use, these products bring **significant risks** with them. The dangers of excessive big tech use has been **highlighted time and time again** by different expert groups. In 2019 all but one Dutch rectors stated in de Volkskrant that big tech is threatening our universities and it is time to draw a line. The "Cyber Security Raad", "Autoriteit Persoonsgegevens" , "Tweede Kamer" and "Clingendael institute" all shared similar messages. This shows that the subject is highly relevant, but looking closer at the IT landscape of Dutch universities reveals **minimal change**.

This report aims to inform decision makers on what the industry sees as the biggest risks regarding big tech use and how these risks can be mitigated. We conducted a total of **11 interviews** with professionals and asked them to rank the current risks regarding big tech use, and to propose mitigations. We put the findings of these interviews in context of recent reports. We learned that three risks are seen as most important. First, a **loss of academic freedom and digital sovereignty**. We highlight that digital sovereignty is important for a strong negotiation position and that academic freedom can be tainted by big tech. Second is **privacy issues**. We show that the products of big tech companies can have high privacy risks, which have been highlighted by DPIAs and mitigated after extensive collaborations. The third most important risk is **vendor lock-in**, which we highlight with examples on Blackboard or Osiris. Furthermore, we make the comparison between big tech's dominance and the dominance of academic publishing companies, which shows that vendor lock-in can be a real problem.

During our interviews we discussed several **mitigations**. Most importantly is the **use and development of more (and better) alternatives**. These alternatives lessen the current monopoly by big tech which leads to more digital sovereignty and reduces vendor lock-in. A second important theme in our solutions is **awareness**, which can contribute to more people using and promoting alternatives. The final mitigation centers around keeping big tech **accountable** by means of EU law, which mitigates privacy risks. The research & education sector should also be more vigilant and include public values higher into their decision making process.

Although SURF has several initiatives based on digital values, there are still many **opportunities for improvement**. By implementing the recommendations the sector will lessen the risks mentioned above, making them more resilient in this digital age.

*Quote from Bart Jacobs in one of the interviews

1 Introduction

In 2019 the rectors of all but one Dutch universities published a letter, stating that our dependence on big tech companies has increased and is threatening our universities.[1] Time to draw a line, they wrote. Almost two years later, in 2021, 19 Dutch professors in cyber security and related fields signed a letter stating that not much has changed.[2] According to their perspective, big tech still posed various risks in different domains, including privacy and security, finance, and ethics. Around the same time the "Cyber Security Raad" published a report stating that the digital autonomy of The Netherlands is under pressure.[3] In 2023 the "tweede kamer" passed a motion calling for research into public-value based digital alternatives for education.[4] Recently the "Autoriteit persoonsgegevens" also mentioned the dependency the education sector has on large tech vendors and how this causes problems[5] and a Clingendael report stated that European alternatives to big tech products are desperately needed to reduce cloud vulnerabilities.[6] All of these letters show that big tech in education is an important topic, but tangible results are still hard to find in the research & education sector. Although the letter from the rectors resulted in a working group, which resulted in an advice report commissioned by the umbrella association Universities of Netherlands (UNL), one of its authors stated in an interview that the this UNL advice report had zero noticeable impact.

Our advice report has several recommendations to SURF and its members. SURF is a cooperative association of Dutch educational and research institutions, that work together to acquire or develop digital services, and to encourage knowledge sharing. This is why they are essential in this report, as they have the perfect position to promote change. A few years ago, SURF launched a public values program which currently employs two experts. This program has undertaken initiatives such as clarifying public values or establishing pilots. Despite the power big tech currently has, there are still new opportunities to regain autonomy. Why is there, even though there is so much talk about this issue, little tangible result? Decreasing big tech reliance is difficult, but possible. One piece of the puzzle is to move away from big cloud providers. CERN has attempted this with their MALT project and learned valuable lessons.[7] 37Signals, a medium sized software company, has shown that it is indeed possible and their "cloud repatriation" project has resulted in considerable cost savings.[8] Cloud repatriation is a recent movement in which companies migrate back to on-premise hosting. As evidenced by the letters mentioned in the beginning, the influence of big tech on education garners significant attention. However, the present IT landscape in universities reveals minimal change.

Given this lack of tangible outcomes, there is a pressing need to gain insight into professionals' perspectives on the risks and mitigations associated with big tech use. Currently there is little known about what the risks actually are or which risks are seen as most important. This is highly relevant, as without this insight it becomes difficult to comprehensively address and mitigate the potential hazards posed by big tech. By engaging professionals directly and soliciting their perspectives on the perceived risks and their relative importance, we aim to fill this gap in understanding, thereby empowering stakeholders to develop more targeted strategies for risk management and regulation in the realm of big tech. In our research we have conducted 11 in-depth interviews with a diverse group of professionals: SURF experts, academics, and university CISOs/CIOs. We consulted these professionals on the importance of different risks and talked about possible mitigations, learning from their ideas. We analyzed this data and put the findings in context of recent news items, incidents and reports. In this report we present a ranking of risks and associated mitigations, while providing specific recommendations. This report aims to add valuable knowledge to the decision making process in universities' IT procurement strategies.

[1] https://www.volkskrant.nl/columns-opinie/digitalisering-bedreigt-onze-universiteit-het-is-tijd-om-een-grens-te-trekken~bff87dc9/

[2] https://accss.nl/podium/open-brieven/overstappen-naar-de-cloud-bezint-eer-ge-begint/

[3] https://www.cybersecurityraad.nl/actueel/nieuws/2021/05/14/%E2%80%98digitale-autonomie-nederland-staat-onder-druk%E2%80%99

[4] https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2023Z08804&did=2023D21124

[5] https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023

[6] https://www.clingendael.org/sites/default/files/2024-02/Policy_brief_Cloud_sovereignty.pdf

[7] https://home.cern/news/news/computing/three-year-malt-project-comes-close

[8] https://world.hey.com/dhh/the-big-cloud-exit-faq-20274010

2 What is currently happening

Public values are mentioned several times in SURF's strategy document 2022-2027.[9] The document states that the sector should remain autonomous from big tech and that public values and sovereignty are essential. We see this strategy reflected in several ways. SURF is proposing to start an **innovation zone on digital sovereignty**. This zone is a response on the advice report[10] UNL published and could serve as an umbrella for several different activities based on digital sovereignty or public values. SURF has also recently launched a **vendor compliance** service. This service aims to hold big vendors accountable to privacy and security legislation and is a proven tool against big tech privacy violations.[11] Another initiative SURF is launching is the **Open Source Program Office** (OSPO). The OSPO is a knowledge and expertise centre for open source software which aims to give substance to public values such as autonomy or privacy. By organising open source knowledge in one central community the OSPO will further the knowledge for open source in higher education. A final way that we recognize this topic returning is on the **strategic agenda for the CSC-wo council**, which is a council that includes decision makers on universities' IT strategy. On the strategic agenda of the CSC-wo council we see that public values is mentioned on the first place. This sound promising, but the agenda point does not seem to translate into objective action. Furthermore, although these initiatives exist, the universities are currently still locked into big tech's products, partly due to SURF's collaborations with big tech.

Outside of SURF the topic of digital sovereignty is also getting more attention. The universities of Groningen, Amsterdam and Utrecht all have programs regarding data sovereignty or public values. When we look at politics, both the EU and Dutch government also aim for a more sovereign IT infrastructure. In European context, we see initiatives such as Gaia-X[12] or International Data Spaces[13], projects that aim to increase European digital sovereignty. Many other companies, such as Moodle[14] or Nextcloud[15], aim for the same. The European Commission has stated in their priorities for 2019-2024 that their digital sovereignty should be strengthened.[16] The Netherlands has an "open, unless"[17] policy, which means that the software the Dutch government uses is as much open source as possible. The education sector does not have such a policy, one of our interviewees suggested that this policy could be a serious option worth exploring.

3 Risks

Every single person we interviewed agreed: big tech in education poses a problem. However, each group of experts seems to have different opinions on what the biggest risk is. While SURF experts and CISOs value privacy most, academics are more focused on ethical risks such as the loss of academic freedom and digital sovereignty. This seems to be a difference between practical versus ideological motivations. In the following section we will highlight the most important risks, as ranked by these professionals, and give specific examples of recent occurrences.

3.1 Loss of academic freedom and digital sovereignty

The aggregated data from all interviewees rank loss of academic freedom and digital sovereignty as the most important risk. The experts working on public values at SURF stated that digital sovereignty is the basis of all other values: if you have no digital sovereignty you have no negotiation position, which decreases digital autonomy. Other academic researchers that we interviewed agree with this sentiment. These researchers believe that we are currently experiencing a large loss of academic freedom and digital sovereignty. In the course of the interviews, however, we learned that

[9] https://www.surf.nl/files/2022-03/surf-strategy-2022-2027-pv-en_0_0.pdf
[10] https://www.universiteitenvannederland.nl/files/publications/Advies%20werkgroep%20publieke%20waarden%20onderwijs.pdf
[11] https://www.nytimes.com/2023/01/18/technology/Dutch-school-privacy-google-microsoft-zoom.html
[12] https://gaia-x.eu/
[13] https://internationaldataspaces.org/
[14] https://moodle.com/
[15] https://nextcloud.com/
[16] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en
[17] https://opensource.pleio.nl/

some people have a different view on this risk. One CISO stated that big tech's dominance is not an issue. However, recent news stories mentioned in the next paragraph show that this risk is very real.

In regards to digital sovereignty, the University of Amsterdam recently stated that "preserving digital sovereignty of universities and researchers is key to a successful digital transformation of the university sector".[18] The UvA published similar research as ours, which investigates digital sovereignty at universities and suggests recommendations. These recommendations[19] and research are worth exploring, via the footnotes below. A recent TNO report also argues for the importance of digital sovereignty in our increasingly automated world, highlighting the problem by stating that "more than 90 per cent of Western data is already hosted in the US."[20] With regards to the loss of academic freedom, there have been multiple examples of big tech deteriorating this in the last few years. In 2020, Zoom blocked a lecture at San Francisco University's College which planned to invite a Palestinian activist.[21] This happened after an Israeli think tank pressured Zoom to drop this talk, citing legal concerns. In 2021, Google fired one of its researchers after she wanted to publicize a critical paper about bias in artificial intelligence.[22] Finally, in 2023, a Harvard researcher in disinformation claimed she was fired after Harvard received a $500 million donation from Meta.[23] All these stories show that big tech can touch the academic freedoms that everyone holds so dear.

3.2 Privacy issues

When considering big tech risks, privacy problems are often at the top of the list, during our interviews they were ranked second in importance. It was mentioned in the interviews that privacy issues affect people personally, which is one reason why some deemed it this important. Big tech is in the market of (personal) data, which can result in data scandals like Cambridge Analytica. SURF, in different capacities together with the Ministry of Justice & Security and SIVON, organised Data Protection Impact Assessments (DPIAs) and Data Transfer Impact Assessments (DTIAs). These DPIAs/DTIAs revealed several privacy issues, issues that would most likely still exist had these organisations not organised the DPIAs/DTIAs. For Zoom, one of the 9 high risk issues was that many personal data were automatically transferred to servers based in the USA.[24] For Microsoft, the high risk that was found (among with several lower risks) was that US law enforcement and secret services could possibly access very sensitive and special categories of personal data.[25] Even though the servers were based in the EU, US legislation made it so that access to these data could be ordered. These issues have currently been addressed with the help of DPIAs and DTIAs. However, a current Schrems-3 court case shows that even the newest EU-US privacy framework might not be sufficient enough.[26] Furthermore, the fact that these kind of risks existed before the assessments were performed shows that big tech can have serious privacy problems. In their defense, during our interviews we got told that some big tech companies do care about what information is given to government agencies.

3.3 Vendor lock-in

Vendor lock-in was rated as the third most important risk by the professionals. According to one of the CISOs we interviewed big tech has us "by the balls", since the tech stack of universities contains so many big tech products that moving away from them will be difficult and expensive. In a vendor lock-in, large companies have the option to arbitrarily increase prices or change agreements since universities have no viable alternative. Dutch vendor lock-in cases in the educational sector include

[18] https://www.uva.nl/en/about-the-uva/policy-and-regulations/general/preserving-digital-sovereignty-of-universities-and-researchers/preserving-digital-sovereignty-of-universities-and-researchers.html

[19] https://www.uva.nl/shared-content/uva/en/news/news/2023/12/new-uva-research-lab-puts-responsible-ai-into-practice.html

[20] https://www.tno.nl/en/newsroom/insights/2022/06/strengthening-digital-sovereignty-makes/

[21] https://www.npr.org/2020/11/23/937336309/welcome-to-the-party-zoom-video-apps-rules-lead-to-accusations-of-censorship

[22] https://www.wired.com/story/google-timnit-gebru-ai-what-really-happened/

[23] https://www.theguardian.com/technology/2023/dec/04/facebook-harvard-joan-donovan

[24] https://www.surf.nl/files/2022-03/dpia-zoom-25-february-2022_0.pdf

[25] https://open.overheid.nl/documenten/ronl-06f045ed745d9540ec4262a6079e8e73ad262a43/pdf

[26] https://shardsecure.com/blog/schrems-iii-prepared

Blackboard, where users were required to pay for data removal, and Osiris, which was acquired by an American investor, resulting in discontinued support and additional vendor lock-in issues.[27] SURF has seen that some companies have tried to increase the prices, but there have not been any drastic measures such as forced prices increases or policy changes. This could make it tempting to believe that vendor lock-in is a non-issue. However, comparing with academic publishers we see that vendor lock-in is a very real and dangerous problem. Some companies in the academic publishing world hold so much power that they have started asking exorbitant prices for access to their journals.[28] Despite universities' efforts towards open access, they have yet to fully disentangle from vendors who impose steep prices, limiting the publication of research outside their proprietary systems. The dominance of these publishing companies and the extreme prices they are asking should serve as a stark warning that vendor lock-in is a realistic danger. When left unchecked the open market can (and probably will) take full advantage.

3.4 Additional risks

The above mentioned three risks are ranked as most important by our interview group, but some other risks have also been mentioned by the professionals in our interviews. First, several interviewees mentioned a **geopolitical risk**. Geopolitics has been mentioned multiple times during our interviews as an issue that the Dutch universities could face in regards to their use of big-tech products. This geopolitical risk has two sides. First, as Europe we are increasingly dependent on the United States for our tech products. Especially if these products are cloud based, the US government can decide much using the US Cloud Act (which states that intelligence agencies can compel US companies to provide requested data, even if this data is not stored in the US). In times where new US leadership could prove to be challenging, we should strive to decrease our dependency. The EU and Dutch parliaments agree, digital sovereignty is an increasingly important topic on their agendas.[29] Second, some interviewees alluded to substantial problems with researchers or students from countries such as China or Iran, who should not have access to sensitive research data about topics such as quantum or nanotechnology. Managing this problem using big tech products has proven to be a real issue.

The following risks were also mentioned in interviews. First, with the increase of cloud based providers, there is a certain **loss of technological knowledge**. There are less and less people who know exactly how their IT systems work because big tech takes care of all the details. Another problem is that big tech gains **life long customers** by using their products on universities. It is possible that students are only familiar with SPSS for example, while R is a perfectly fine alternative. This can coerce students to keep using a certain product, not knowing that there are plenty of good alternatives. Last but not least, big tech is increasingly incorporating AI in its products. Because of the lack of transparency and the **closed nature of AI**, we are unaware how AI is influencing written text or decision making.

Jitsi case study:

> Jitsi was an open-source and self hosted video conferencing platform that SURF offered before the corona crisis. It checked all the public value check marks and the users were very positive about Jitsi. However, the decision was made to not continue the pilot. This decision was made by the IT directors of the universities in the haste of the Covid-19 crisis, something big tech used all to well to their advantage.

[27] https://www.scienceguide.nl/2022/11/edtech-startups-kunnen-oplossing-zijn-voor-problemen-met-big-tech/

[28] https://www.scienceguide.nl/2020/06/vooral-elsevier-profiteert-van-nieuwe-open-science-deal/

[29] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

4 Mitigations

In the previous sections, we illustrated that big tech still poses various real and dangerous risks to Dutch universities. Risks that deserve to be addressed. We currently find ourselves in a position where change is hard to create, but not impossible. In this section we will highlight possible mitigations, some issues with these mitigations, and how these issues can be solved.

4.1 More (and better) alternatives

Alternatives to big tech products increase our digital autonomy and our freedom of choice. These alternatives are software products from other companies than big tech, preferably European and focused on public values such as privacy or data autonomy. Almost all our interviewees agree that freedom of choice is very important. Even though a multi-vendor strategy (in which alternatives are also supported) can be expensive, it seems absolutely necessary when freedom of choice is seen as critical. This multi-vendor strategy should be a two-fold approach. First, SURF should increase partnerships with public-value-focused companies such as Jitsi, Nextcloud or Moodle. Stimulating partnerships ensures a better and more balanced market where it is easier to choose a different provider than the standard. By exploring collaborations with promising companies, SURF can request features or changes in products that benefit SURF members. An important use case for these public-value-focused companies is the research sector. Current big tech products do not provide easy collaboration options between universities, which is something Nextcloud could provide. This was noted after the SURF Nextcloud pilot, which stated that cross-institutional collaboration was the most popular use case.[30] Simultaneously SURF should continue to develop their own products, such as SURFdrive or SURFconext. All of these alternatives increase the universities digital autonomy. The public value experts at SURF stated that even if a service is not used very often, it can still contribute to more freedom of choice and a higher digital autonomy.

One of the downsides of this strategy is that maintaining alternatives is expensive, especially at the start. There are less people who know how to operate these alternatives which gives higher starting costs. This can be solved, people can be trained. Additionally, using alternatives ensures you are no longer in a vendor lock-in, which decreases the risk of big tech arbitrarily increasing prices. To further reduce costs of alternatives, SURF should find partnerships with other organisations that can share in development or procurement costs. Partnerships are necessary since big tech has more budget and time than any one country or organisation can spend on development. These partnerships are worth exploring on a European level with organisations such as GÉANT and the Digital Europe Programme, or on a national level with organisations such as NPULS, SIDN, or governmental organisations. Another downside we heard in the interviews is that the products are usually less user-friendly, but this does not mean that this approach should not be explored. These alternatives are still highly appreciated by more privacy sensitive employees of universities. More importantly, as stated earlier, partnerships with public-value-focused companies can ensure more or better features in alternative products. Because these alternatives are often open source it is must easier to request features, or even add them yourself. Finally, a problem that is inherent to SURF's structure is that the members of SURF are the ones who decide what projects and services SURF focuses on. Even if SURF would like to have more alternatives, in the end, SURF's members have to agree with everything SURF decides. This was made painfully clear with the Jitsi use case, explained previously. We delve deeper into this topic in the next section, discussing awareness.

4.1.1 Concrete recommendations

1. Make the decision to dedicate at least 2-5% of SURF's (Trust & Security) development budget to specific open-source projects. These projects should have actual use cases for SURF's members. Alternatively another budget can be used, but having a predefined budget helps.

2. SURF starts the scaled-up Nextcloud testing ground, as the previous pilot had promising results. Additionally SURF can learn from universities such as Nantes, Twente or TU Berlin, as they all use Nextcloud in a successful manner.

[30] `https://www.surf.nl/en/news/own-your-data-with-open-source-collaboration-platform`

3. SURF should launch more pilots on public value based programs. These could be Moodle as an alternative of Brightspace, Jitsi as an alternative to Microsoft Teams, GIMP as an alternative to Adobe Photoshop or R as an alternative to SPSS.

4. SURF should investigate the option to collaborate with funding programs such as the Digital Europe Programme or national governmental funds in order to improve alternatives. This is necessary since the research & education sector does not have the same funds or capacities as big tech.

5. Universities should investigate the use of alternative platforms for researchers. A platform such as Nextcloud can have better collaboration options between universities. If this yields positive results, universities should embrace alternatives even more.

6. SURF should investigate the option to collaborate with GÉANT in developing and maintaining big tech alternatives. Many NREN's have their own scheduling tools, meeting tools, etc. This could be centralized where each NREN is responsible for their own tool.

7. In order to improve the amount of experts for alternatives on big tech, SURF should organise public values based workshops on how to operate these platforms. This helps to increase the knowledge on alternatives: for example, there are currently many more Microsoft experts than there are Nextcloud experts.

4.2 Awareness

As shown with the Jitsi example, SURF's structure makes it harder to push decisions that are not optimal in a financial sense. By increasing awareness and understanding of this topic, decision-makers can choose alternatives instead of always opting for big tech. That is why SURF should focus much more on raising awareness about public values and digital sovereignty, which shows its members the importance. By sounding the alarm on this subject more clearly SURF can garner attention regarding the current issues of big tech. If more people inside the organisation of a university become aware of these issues, change is more likely. This awareness must happen on all levels of a university. The students, professors, general employees and the executive board should all be made aware of the problems. Furthermore, politicians and members of overarching bodies such as "Universiteiten van Nederland" (UNL) should be better informed about the risks. Solutions in this area can be broad, anything from media attention to an open-source training to notifying student councils. This in turn will ensure that the members of SURF see the necessity of alternatives and agree on development of new tools or partnerships with these public value based platforms.

4.2.1 Concrete recommendations

1. Garner more media attention for this problem. For example, articles posted on ScienceGuide, AG Connect or de Volkskrant (follow-up 2019 article). Additionally a podcast, articles or videos on SURF's website will help.

2. SURF employees have different views on this topic. In order to create more support of the alternatives to big tech, SURF can organise roundtable discussions to exchange opinions about this topic.

3. Promote this topic in university settings. This subject could be brought to attention by contacting the university newspapers, the "Interstedelijk Studenten Overleg" (whose position on digitisation currently does not mention digital sovereignty), UNL, or the university's student councils.

4.3 Keep big tech accountable

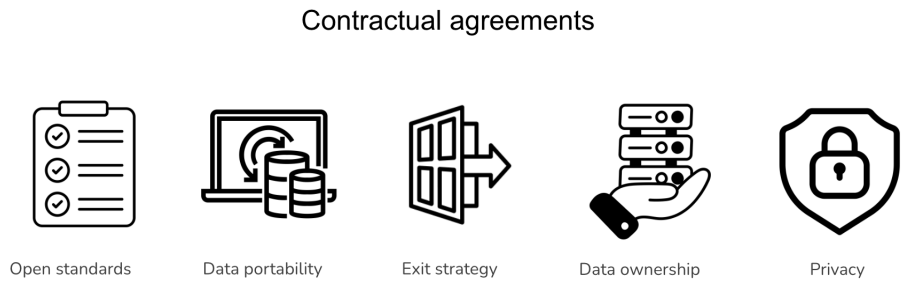
One of the topics that constantly emerged during the interviews is that we should not ignore big tech. Big tech simply exist and they own a very large market share. However, we can make changes to prevent them having the upper hand. SURF has achieved real change in big tech by using DPIAs to hold these companies accountable.[31] This helps the cause. Furthermore, SURF is a large cooperation, which gives it the power of combined strength, which provides some leverage. This leverage can be utilized for positive contractual agreements, such as (free) data extraction upon contract termination or more thorough privacy settings. The image below shows some of the topics on which contracts can be designed. These agreements can reduce vendor lock-in and increase privacy for the end users.

This solution also requires a two-fold approach. On one hand, SURF should design contracts with the above-mentioned risks and public values in consideration. Exploring options to include agreements about open standards, exit strategy, data ownership, or privacy protections in the contracts is also essential for a new approach. On the other hand, SURF has to make sure that big tech complies with EU regulations such as the GDPR, Schrems-II, or the DMA. In this aspect SURF is making progress: due to the recent launch of a new service called "SURF vendor compliance", this topic gets the attention it deserves.

Universities also have to be more vigilant. Although the rectors signed the 2019 letter stating that it is time to draw a line, the universities kept on growing their big tech dependence. If they still stand with the statements from 2019, their words need to be translated into action. Specifically, the public value commitment made in 2019 should be made tangible by including public values into their IT procurement & risk strategies. This is actually one of the three recommendations the UNL advice rapport made in 2021. Other recommendations stated that the universities should take a leading role in a common vision about public values in education, highlighting the issue in their own institution, the education sector, the government and in Europe. The other recommendation that was made to universities was that their ambitions regarding public values should be cemented in a Declaration. This is a document which explicitly states why and how public values are used as a starting point for their IT related choices. Unfortunately these recommendations have not been implemented as of yet, something we urge the universities to do.

4.3.1 Concrete recommendations

1. Investigate the option for stricter contractual agreements about:
   (a) Open standards (Can Microsoft products "speak" with open source products?)
   (b) Data portability (Can my data be moved freely between different systems?)
   (c) Termination & exit strategies (How expensive is it to switch vendor or terminate the current contract?)
   (d) Data ownership (Who owns the data?)
   (e) Privacy protections (Where is the data stored? What do the DPIAs/DTIAs tell us?)



[32]

[31] https://www.nytimes.com/2023/01/18/technology/Dutch-school-privacy-google-microsoft-zoom.html
[32] Icons from Noun Project, from left to right: Soremba, WiStudio, Andi Nur Abdillah, Design Circle, Nursila

2. Expand the vendor compliance service, with more people there is more capacity to investigate important companies.

3. Universities should articulate their public values commitment within their IT procurement strategy. Furthermore, they should take the UNL advice seriously and implement recommendations 4 and 5.

4.4 Additional mitigation strategies

In addition to the previously mentioned mitigation strategies, there are several other (smaller) ideas that surfaced during the interviews. Many of our interviewees agreed that real change can be enforced by way of **European legislation**. In previous years we have seen this happen with the GDPR, and currently with the DMA, legal frameworks which provide real change. A recommendation is that SURF should keep the politicians aware of all these mentioned risks, which could help with new legislation. By way of lobbying and speaking about the issues with decision makers, SURF could make politicians (both national and European) more aware of the risks.

Some of our interviewees spoke about **breaking up big tech**, in a European and a United States counterpart. On a first glance this idea might seem like a bit much, but it could actually work. These different counterparts could each operate based on different values, and could thus make their products work differently based on these values. However, this mitigation strategy is too complex for the research & education sector and hence out of scope of this paper.

5 Conclusion

Mitigating all risks mentioned in this report is a large and complex problem. We have attempted to provide one single document that highlights the risks and possible mitigations, while providing realistic perspective for action. However, solving the larger problem is not as simple as implementing a few bullet points. It requires a strong culture shift in both the universities and in SURF, in which free and open software is seen as a real option and public values are taken more seriously. This takes time.

We have shown that this culture shift is necessary. Almost all Dutch rectors, many cyber professors, and even the national "Cyber Security Raad" have highlighted either the need for digital sovereignty or the dangers of using large cloud providers in universities. Also the "Autoriteit Persoonsgegevens" and the "tweede kamer" highlighted this problem previously. Time and time again, important groups mention the problem. In our report we have illustrated the most important risks, as ranked by the professionals we interviewed. Clearly seen as the leading risk is the loss of academic freedom and digital sovereignty. Examples such as Zoom blocking a lecture or Harvard firing a researcher after a large Meta donation show that big tech can in fact encroach upon our academic freedom. Reports from TNO or the University of Amsterdam also emphasize the importance of digital sovereignty. Additionally, multiple DPIAs have shown that the products universities use daily can have high privacy risks. These risks have been mitigated but the DPIAs show that this issue is very real. Lastly, we compared the rising vendor lock-in of big tech products to the lock-in of the academic publishing world. This comparison demonstrates that while a vendor lock-in may not pose immediate issues, it has the potential to create problems in the future.

All these risks can be solved, or at least mitigated. Our interviewees agree that more and better alternatives is the most important solution. This strengthens our digital digital autonomy and increases our negotiating power. The perfect use case for these alternatives is the research sector. Sharing data or communications between universities can be difficult with traditional products, but is something Nextcloud can do (almost) perfectly. Collaborations with organisations that can spend either money or manpower on this project and collaborations with the companies developing these products should both be explored. Because these products are often open source SURF could influence the development which helps to make the software more suitable for SURF's members. But these members also have to agree with the sentiment about digital sovereignty. This is why we need more awareness on this topic. Using media attention and highlighting this problem internally are just some of the ways to help make members more aware of the risks and mitigations. SURF

should keep explaining why we need alternatives and why the cheapest is not always the best. The final solution we highlighted in detail speaks about keeping big tech accountable. By using DPIAs and contractual agreements SURF can change the way big tech is operating. This has been demonstrated in multiple DPIAs to Zoom, Microsoft and Google and this work is currently continuing with research into other services. **What we need are three A's: Alternatives, Awareness and Accountability**.

Breaking free from big tech is possible. The examples of CERN and 37Signals, which we mentioned in the introduction, illustrate that cloud repatriation can save costs and increase digital autonomy. The possibility to reduce big tech's power exists, but the drive not yet. In all honesty, big tech also offers benefits. It is extremely easy to use, is the de facto standard and is currently relatively cheap. This makes it an easy choice for IT directors. But our current dependence on big tech is too much. The risks are too high. We advocate for smarter choices, with digital sovereignty & public values placed high in the decision making process, not as an after thought.