PRIVACY COMPANY

The GDPR as a means to protect digital sovereignty of universities

Expert memo

Arnold Roosendaal, LLM, PhD

1. Introduction

This is an expert memo, commissioned by the University of Amsterdam, and meant to share expert insights and experiences with the researchers of the University of Amsterdam as input for their project on digital sovereignty of universities. The memo shares insights based on the work provided by Privacy Company, mainly in the context of performing Data Protection Impact Assessments (DPIAs) on tools and applications from large-scale digital technology suppliers.

This memo will start with some background on the contracting practice of large digital services suppliers (section 2) and describe how lock-in effects may influence the digital sovereignty of universities (section 3). Then, the GDPR is presented as a means to (re)gain some control over the processing of personal data for which the university is a data controller (section 4) and in particular how DPIAs can help empower universities to negotiate contracts and have tools or applications changed in such a (technical) way so that they comply with the GDPR (section 5). This leads to the conclusion that the GDPR can be used as an instrument to protect digital sovereignty of universities.

As argued in the research report on the digital sovereignty of universities,[1] universities have a need for "sovereignty" to remain independent in their research activities, education, and their position as academic institutions. With the ongoing technological developments and digitalisation, this sovereignty has gradually become an issue of "digital sovereignty". The notion of "digital sovereignty" is predominantly used as a discursive tool to support a variety of narratives and objectives.[2] For this reason, Meiring a.o.[3] prefer to speak about digital sovereignty *claims*, allowing for different dimensions of digital sovereignty to be discussed.

An important aspect of digital sovereignty is the autonomy of universities vis-à-vis suppliers of digital technologies. While modern universities simply *need* digital technologies to facilitate research and educational activities, and therefore often have to enter into contractual relationships with commercial digital technology suppliers, they still need to retain their independence from these providers.

The use of technology is not a problem in and of itself. However, universities' heavy reliance on digital technologies provided by external suppliers and the limited ability to negotiate contracts and to control the processing of personal data *is* problematic.

[1] Information Law and the Digital Transformation of the University, Part I. Digital Sovereignty (https://www.ivir.nl/part-i-digital-sovereignty/) & Part II. Access to Data for Research , University of Amsterdam, Institute for Information Law 2023 (https://www.ivir.nl/part-ii-access-to-data-for-research/).

[2] Meiring, A., and others, "Information Law and the Digital Transformation of the University: Digital Sovereignty, Data Governance and Researchers' Access to Data. Part I. Digital Sovereignty", University of Amsterdam, Institute for Information Law 2023, p. 7.

[3] Ibid.

The General Data Protection Regulation[4] (GDPR) provides requirements for the legitimate processing of personal data. Basic principles include transparency, facilitating rights of data subjects, and data minimisation. In cases where the processing of personal data is likely to involve a high risk for the rights and freedoms of individual data subjects, the performance of a DPIA is mandatory.[5]. This paper describes how the GDPR, and in particular DPIAs, can be used as an instrument to improve the digital sovereignty of universities in their relations and negotiations with digital technology suppliers.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] Article 35 GDPR.

2. Background on digital services contracting

Over the past decades, the use of technology and digitalisation has increased enormously. Today, digital technology and software applications are widely used to support human activities. This also holds for the work at universities, where staff is supported by software to prepare courses and to register student information, and researchers use applications to collect and analyse data and to draft reports. In other words, universities participate in digital and data-driven environments.

Due to the increase of data usage, services that support the work of researchers have to work at a large scale. They also need long-term maintenance so as to prevent frequent changes of services and tools. The type of applications that have the necessary scale, stability, and maintenance is usually provided by large-scale software suppliers. These suppliers have ample resources to develop and maintain applications that can be used for a wide range of activities. The development of complex software systems, in particular with applications that can interact, is costly and time-consuming. For this reason, the sustainability of software applications depends on large-scale sales and usage. The more users of a certain application, the more the costs are spread. In order to gain a large user community, international provision of the services is necessary. Besides, the services as such have to be as standardized as possible, since individual tweaks are relatively expensive.

Like digital services are standardized, the same applies to the accompanying contractual arrangements. Instead of negotiating the business contracts with each and every customer, digital service suppliers make use of standard contracts and standard terms and conditions (or Terms of Use/Service) when selling their software. For business contracts, there is usually an Enterprise Agreement available online that is referred to in the commercial contract, which specifies the licenses and services an organisation purchases. In both cases, concluding a contract to use a service implies accepting standard terms and conditions, as well as all any other conditions mentioned in the agreement itself.

Contractual terms tend to be lengthy, full of legal sentences, and contain all sorts of rights or claims to the benefit of the digital service supplier. What exactly the scope and meaning of these rights and claims is, is usually difficult to understand. Besides, the contracts often have cross-references or links to other contracts and terms that may also apply depending on the type of service at hand. The contract structure for using services may thus become large and complex.

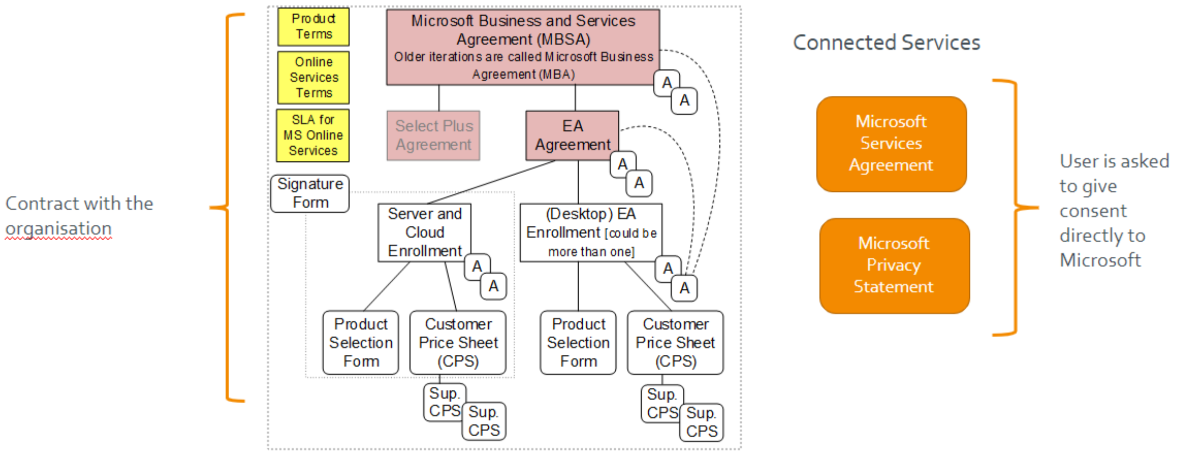

Contract with the organisation
Product Terms
Online Services Terms
SLA for MS Online Services
Signature Form
Microsoft Business and Services Agreement (MBSA)
Older iterations are called Microsoft Business Agreement (MBA)
A
A
Select Plus Agreement
EA Agreement
A
A
Server and Cloud Enrollment
A
A
(Desktop) EA Enrollment [could be more than one]
A
A
Product Selection Form
Customer Price Sheet (CPS)
Product Selection Form
Customer Price Sheet (CPS)
Sup. CPS
Sup. CPS
Sup. CPS
Sup. CPS
Connected Services
Microsoft Services Agreement
Microsoft Privacy Statement
User is asked to give consent directly to Microsoft

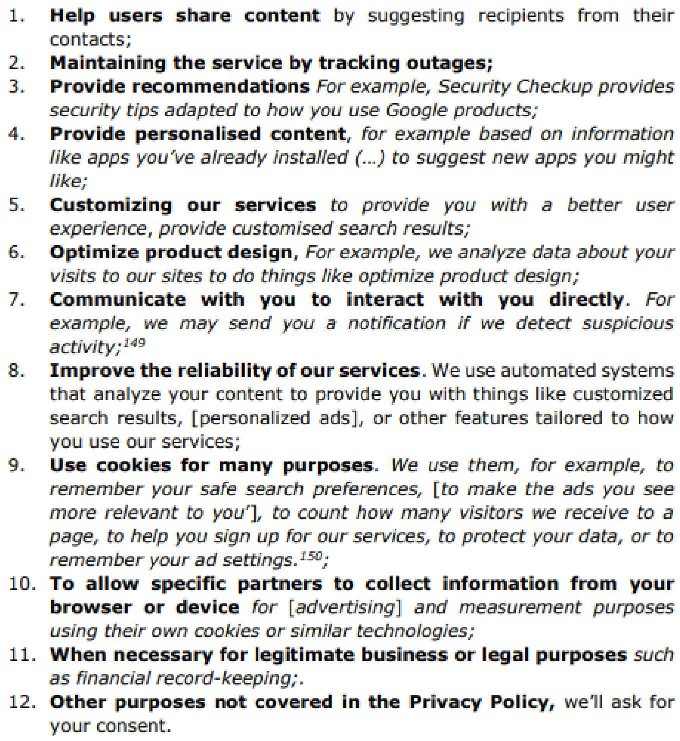
Figure 1: Contract structure of Microsoft Office 365[6]

The effect of the way contracts and terms of service are structured and presented is that organisations can barely understand what it means to use the services for their data. Data processing purposes are typically not transparent; there is an information asymmetry between users and suppliers. Moreover, given the powerful position of large-scale software suppliers, the contracts are often non-negotiable.

In the context of a university, the end-users of software can be scientific and educational staff members, but also support staff such as system administrators, and of course students. They are all affected and bound by a contract concluded by the university. Other people whose data can be processed are people who for example participate in scientific research. For all those categories of data subjects, universities have a responsibility to properly protect their personal data and to ensure that all data processing activities are GDPR compliant. Since suppliers are not always transparent, this can be very hard for a university – in its capacity as data controller – as it may not be able to properly inform data subjects about the processing of their personal data.

Figure 2 below shows how the self-defined purposes of suppliers may include commercial data use and improvement of services. Data analysis can make the products better and more attractive, but at the same time increases the power position of the supplier. Moreover, it is well-known that also diagnostic data, which often also include personal data, are used by the supplier for its own purposes. This makes the supplier a data controller for some of the processing activities, thus limiting the control of the university, which the supplier should only be serving as a data processor. The definition of purposes by a supplier as a processor may also be illegitimate or result in a factual situation of 'joint controllership' with the university. Both scenarios are not desirable.

[6] See: Privacy Company 2019, DPIA Office ProPlus, version 1905.



1. **Help users share content** by suggesting recipients from their contacts;
2. **Maintaining the service by tracking outages;**
3. **Provide recommendations** *For example, Security Checkup provides security tips adapted to how you use Google products;*
4. **Provide personalised content**, *for example based on information like apps you've already installed (…) to suggest new apps you might like;*
5. **Customizing our services** *to provide you with a better user experience, provide customised search results;*
6. **Optimize product design**, *For example, we analyze data about your visits to our sites to do things like optimize product design;*
7. **Communicate with you to interact with you directly**. *For example, we may send you a notification if we detect suspicious activity;*[149]
8. **Improve the reliability of our services**. We use automated systems that analyze your content to provide you with things like customized search results, [personalized ads], or other features tailored to how you use our services;
9. **Use cookies for many purposes**. *We use them, for example, to remember your safe search preferences, [to make the ads you see more relevant to you'], to count how many visitors we receive to a page, to help you sign up for our services, to protect your data, or to remember your ad settings.*[150]*;*
10. **To allow specific partners to collect information from your browser or device** *for [advertising] and measurement purposes using their own cookies or similar technologies;*
11. **When necessary for legitimate business or legal purposes** *such as financial record-keeping;.*
12. **Other purposes not covered in the Privacy Policy,** we'll ask for your consent.

Figure 2: Example of purposes for processing of diagnostic data in Google G-Suite

Software services used by universities are often provided in packages of related or interconnected applications. M365, for instance, contains the widely used Microsoft Office suite (including Word, PowerPoint, Excel, Outlook Exchange), collaboration tools, and cloud storage. It also facilitates connections with LinkedIn. By providing a number of services that cover different needs and functionalities, while also connecting those, a "lock-in" effect is created. As unbundling of a suite of digital services and switching between service providers are difficult, the user becomes dependent on the supplier: locked-in. A hindering factor in this regard is that the technical interaction between applications from different suppliers is usually not as smooth as the interaction between comparable tools offered by a single supplier.

Finally, most of the large-scale suppliers of software (suites) originate from the United States. They have offices in the EU as well, and because they provide their services in the EU and process personal data of EU citizens, they fall within the scope of the GDPR. This offers some protection to the data subjects whose data are processed when using the software products. However, often personal data are transferred to US entities of the supplier. Moreover, even when the data are processed within the EU (European data centers), there are risks of US government agencies demanding access to the data.

3. Dealing with lock-in effects

As described in the previous section, there are a number of factors that contribute to the emergence of lock-ins. This section will describe the different ways a university can deal with lock-in effects since simply accepting these effects may challenge the digital sovereignty of universities in various ways . For example, the freedom of choice regarding digital applications can be limited, and data that are stored in one application may not easily be transferrable to other applications. Furthermore, the integration of tools in software suites increases the interdependence between applications and a user's professional activities.

Importantly, digital applications may not be fully GDPR compliant, with the result that lock-ins with suppliers can impede universities' legal compliance. Universities should therefore make an inventory of the digital tools necessary to support their activities as well as their accompanying suppliers. Such an overview will show which suppliers have a dominant or key position in the market. Especially the dominant suppliers on which universities are most dependent have to be GDPR compliant – otherwise universities cannot live up to the legal obligations that are imposed on them as data controllers.

For universities, there are a few options available to (re)gain digital sovereignty in relation to large-scale software suppliers. Of course, they can try to leave and switch to an alternative supplier or try to built tools or applications themselves. Or – and this is perhaps a less known strategy – they can try to make the dominant supplier compliant with the GDPR and establish more control and transparency, which in turn contributes to their digital sovereignty.

3.1. Switching to an alternative

Switching to an alternative (commercial) service provider is not as easy as it seems. Even though the large-scale digital service suppliers allow customers to switch in their 'take it or leave it' standard contracts, they know that the chance of an organisation leaving them is small. Obviously, this is a direct result of the lock-in effects and their power position as described above. When users leave for an alternative supplier, issues may arise concerning interoperability, the format in which data can be downloaded from the original platform, and collaboration with academic peers from other universities that have not made the same switch. Moreover, alternative software may be relatively expensive when the number of users is not as high and the costs of development and maintenance are therefore relatively high as well. For many software tools, an "alternative" often means that another supplier is selected that is comparable to the current supplier, which will usually not solve the issue of non-compliance with the GDPR and the lack of sovereignty over the data processing. Another implication may be a loss of functionality. So, an alternative supplier for a similar kind of software may not be a real alternative in practice.

3.2. Build your own alternative?

When there is no appropriate alternative available, another option is to investigate whether it is possible to build the alternative service yourself. The 'yourself' in this respect can be a collaboration of universities. A good example is the cloud offered by the Dutch SURF foundation to host software and provide storage. For tools that are widely used by educational institutions, it may be worthwhile to develop sector-owned alternatives. The feasibility of this effort depends on the complexity of the software. It is not likely that self-developed software tools will possess the degree of interoperability that is available with the tools provided by large-scale software suppliers. Nevertheless, it is worthwhile to think about what tools can be replaced without frustrating ongoing activities so as to improve the digital sovereignty of universities. It must however be noted that building your own alternative software tools requires time and money, and that not all current tools can be replaced easily. When universities cannot build there own alternative and depend on external suppliers, the remaining option is to insist on the supplier becoming compliant.

3.3. Insist on compliance with the GDPR

The third option of (re)gaining control is to insist that the supplier demonstrates its services are GDPR compliant. Insisting that a supplier complies with the GDPR seems like an obvious step but is not as easy as it may seem. A supplier may not be compliant for various reasons. For instance, the supplier is not fully aware of its responsibilities and does not understand the context and applicability of the GDPR. Or, the supplier knows that he is not compliant but has incentives for this, following from the commercial interests that were described earlier. A fine from a supervisory authority can be reduced to a "calculated business risk" that does not outweigh the commercial benefits of non-compliance. However, the risk of a sanction from a supervisory authority is probably not the most important risk for suppliers.

The biggest risk for suppliers is, in fact, the exodus of users from their platforms. Obviously, the utility of data for commercial purposes largely depends on quantity, so the more users of the software or a platform, the more data and insights can be produced. When a couple of thousand users decide to leave the service, this is typically not that problematic, but when it comes to millions of users leaving, this definitely impacts the position of the supplier. For example, in the early days of social media, the Dutch "Hyves" platform was popular, but ultimately lost its battle with Facebook and had to end its services. More recently, Twitter had to change policies after users criticised the takeover by Elon Musk and many of them left to alternatives such as Mastodon.

Although insisting GDPR compliance is not easy, practice has shown that it can really pay off. The next sections will show how the GDPR can be used by universities as an instrument for taking more control over data processing by suppliers and, by implication, increasing the digital sovereignty of universities.

4. Improve GDPR compliance, harness the contract

The GDPR is a legal framework that sets out clear rules and requirements for the legitimate processing of personal data. As soon as personal data of EU citizens are processed, or personal data are processed in the EU, the GDPR applies and imposes obligations to each entity involved in the data processing activities independently. With significant fines as a risk, compliance with the GDPR has become a topic of relevance in the board room of business users. Universities and other organisations have never felt more urgency to improve their compliance with data protection law.

The use of software can raise quite some data protection issues. These issues can impact the users of the software as well as other people whose data are processed with the help of the software. In the context of a university, the users can be scientific and educational staff members but also support staff such as system administrators. Other people whose data can be processed are people who for example participate in scientific research. In regards to both categories of data subjects, universities have a responsibility to properly protect their personal data and to ensure that all data processing activities are GDPR compliant.

Besides organising the internal compliance of the university itself, universities must also make sure that only GDPR compliant organisations are contracted as processors or joint controllers. The processing of personal data is oftentimes necessary to provide services, so it has to be kept in mind that there will always be personal data available to the software supplier. The increase in cloud-based services only amplifies this. Without suppliers full cooperation, a university, in its capacity as data controller, will not be able to properly inform data subjects about the processing of their personal data. However, requiring large-scale suppliers to comply with the GDPR is not as straightforward as it may seem.

Even though suppliers usually recognise the applicability of the GDPR, they often dispute the qualification of certain data as personal data. According to the GDPR, anonymous data are not personal data, since these cannot be related to an identified or identifiable natural person by any means. A direct effect of data being considered anonymous is that the further processing of these data by the software supplier is not restricted, even when the supplier determines its own purposes of the processing. Hence, qualifying diagnostic data as anonymous is very attractive to software suppliers, as long as the data can still be used for the purposes the supplier has envisaged.

4.1. Relating to an identified or identifiable natural person

For general purposes, such as analytics or statistics, the use of aggregated data is very common. However, when these data are not aggregated at a sufficient level, or when there are possibilities to combine the data or recognize the data as part of a specific interaction with the software, individuals could maybe still be indirectly identified. The threshold for data anonymisation is, in other words, high.[7] Arguments brought forward by software suppliers that they do not intend to identify the individual user do not stand, as the GDPR looks at the *possibility* of identification, not the factual situation. When assessing the possibility of identification, one has to take into account all the means available to the entity that holds the data. Given the nature and technical skills of large-scale software providers, the presence of adequate means to enable identification is not that much of a question. For example, databases that can be used to create the link between other datasets are usually in place (for purposes of application logging and transaction logging) and even mandatory for security reasons. Essentially, the GDPR is typically applicable to the data processing activities performed by large software suppliers.

4.2. Roles and responsibilities for personal data processing

The digital services contract with the supplier has to be in line with the GDPR. Part of this, is that it must provide an overview of the roles and responsibilities of the parties to the contract and has to ensure that the supplier, as a data processor, provides meaningful access to data and support in responding to data subject access requests. The contract should not leave room for the data processor to determine its own purposes for the processing personal data, or, where applicable, there has to be a clear description of joint controllership and the division of responsibilities between the parties.

A data processor that also acts as a data controller constitutes a risk for the university of not being able to comply with the GDPR in its capacity of data controller. In such cases, there is a problem with the data processing agreement (which complements the business agreement), as the agreement does not reflect the factual data processing situation. What happens is that the university loses control over the personal data that are processed on its behalf, while the supplier may not have a legitimate ground for its additional processing purposes. Without instructions, the supplier is in principle not allowed to invoke the legitimate ground that the data controller uses to process personal data or have them processed by a processor.

Of course, large-scale software suppliers have their *own* responsibility to be GDPR compliant when offering their software and services to entities within the EU. Whether they act as processors, joint controllers, or independent controllers is irrelevant in this regard.

Sometimes a supplier offers the user an additional functionality that does not fall under the business agreement. The difficulty is then to prove that illegitimate processing is taking place, especially where the suppliers state to process data anonymously while this is hard to test for data subjects. Pseudonymous data can still be related to individuals, but only indirectly or in combination with other data. Direct identifiers are deleted or replaced by a (random) string of characters, a pseudo-identifier. When different pseudo-identifiers are used for different processing activities it is hard or harder to combine data that relate to the same individual. Nevertheless, “difficult” is not the same as “impossible” and the data involved still qualify as personal data on the processing of which the GDPR is applicable.

[7] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216.

As a result of using additional services, the user is bound to a consumer contract with different terms and conditions than the business agreement. These terms are usually presented via a link with a tick box that the user has to click on before the software can be used. This is, for instance, the case when a user gives permission for some additional (connected) services in Microsoft 365, such as the spelling checker. These (consumer) terms often allow for the processing of much more data about the user than the business agreement does. The software supplier than has more means to influence the behaviour or otherwise impact on the rights and freedoms of the user. The problem is that the data controller (the university) loses control over the data processing by the supplier for certain activities. Besides, the user will not always be aware of this and becomes subjected to additional data protection risks. Ultimately, diversity in applicability of contractual terms depending on specific uses by individuals makes it hard for universities to stay in control over the data processing. They cannot act sovereignly when providing tools to their employees and students to support their daily activities.

5. Data Protection Impact Assessments

The GDPR as such does not prohibit the processing of personal data, but puts in place a number of requirements to be fulfilled for the processing to be legitimate. The GDPR also provides an instrument to make a proper assessment of the processing with a focus on risks for the rights and freedoms of individual data subjects: the Data Protection Impact Assessment (DPIA).

According to Article 28(3)f of the GDPR, a processor has obligations to cooperate with the data controller to fulfil the duties following from the GDPR. This section will zoom in on the DPIA and show how this specific instrument can be of help in forcing digital service suppliers towards compliance. A DPIA has to be performed on data processing activities that are likely to result in a high risk for the rights and freedoms of individuals.[8] The business user, i.e. the university, in its capacity as data controller, is the one to carry out the DPIA. This in turn triggers the supplier's legal obligation as a data processor to cooperate.[9] **This way, a DPIA can be used to influence the behaviour of large-scale software suppliers**. Carrying out a DPIA is time and resource-intensive, but practice has shown that it can be quite impactful to influence the supplier's contract terms and practice. Article 35 of the GDPR sets out when a DPIA is mandatory to perform. There are a few specific examples mentioned, but in general a DPIA is required when a data processing activity is likely to result in a high risk for the rights and freedoms of individuals. The European Data Protection Board (EDPB) has published a list of nine high-risk indicators to decide when a DPIA is mandatory:

- Evaluation or scoring;
- Automated-decision making with legal or similar significant effect;
- Systematic monitoring;
- Sensitive data or data of a highly personal nature;
- Data processed on a large scale;
- Matching or combining datasets;
- Data concerning vulnerable data subjects;
- Innovative use or applying new technological or organisational solutions; and
- Data processing that prevents data subjects from exercising a right or using a service or a contract.[10]

When the processing of personal data implies that two or more of the indicators of the EDPB list are applicable, a DPIA is mandatory. Given that software from large suppliers is used for core activities or services of universities, the processing will probably fulfil the criterion of large-scale processing. Other criteria that often apply are evaluation or scoring (including profiling) for determining personal interests of the users, processing of sensitive data (like health information on students or data subjects involved in research programs), and data concerning vulnerable data subjects

[8] Article 35 GDPR.

[9] In line with article 28(3)f GDPR.

[10] Based on the earlier Article 29 Working Party list (Opinion 248), "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", see: https://ec.europa.eu/newsroom/article29/items/611236 .

(employees). So, in many cases of software use by universities a DPIA is mandatory. In case of doubt, a pre-DPIA can be executed, which looks at a number of indicators for potential high risks, or a DPIA can be performed voluntarily.[11]

The aim of a DPIA is not to prohibit a certain data processing activity, but to determine which risks may be present and what measures, technical and organisational, can be taken to mitigate those risks. A DPIA can, thus, be a good instrument to gain insight in data processing activities. As a data processor, a large-scale software supplier is legally obliged to cooperate in the DPIA process. Without the data processor's help, the data controller will probably not acquire sufficient insights to be able to fulfil its information and transparency duties towards data subjects. And without transparency, the processing activities will be a violation of the core principles of the GDPR and therefore be illegitimate. The data controller then has a "compliance problem".

The GDPR demands both technical and organisational measures to safeguard the protection of personal data. A DPIA can help to determine the relevant measures. The contract is the basis for these compliance safeguards. However, even when data processing activities are compliant and legitimate, there may still be implications for the users. This underlines the importance of not only looking at contracts and compliance on paper, but also at compliance in practice. Are the processing activities indeed in line with what is agreed in the contract? Or are there differences? And is the supplier aware of these differences or not?

Some situations, however, cannot be solved by contract law. The only way to gain as much control as possible is by using technical research as part of the DPIA to discuss the real practice or data processing and to force suppliers to change things where necessary and to reflect this as much as possible in the contract.

5.1. Scope of the Data Protection Impact Assessment

The use of software may entail the processing of several types or categories of personal data. In a university context, this depends on the type of research that is performed. For instance, data about interviewed people can be processed in a text file or a spreadsheet. Usually, software suppliers refer to those data as "content data": the data that are processed in the content of files created by the user. In a so-called Data Processing Addendum (DPA), which typically applies next to a supplier's general Terms & Conditions, the supplier often specifies that the processing of data is limited to such "content data", to the extent necessary to provide the services. Indeed, it is obvious that content data have to be processed when offering (cloud-based) software. However, all processing of *other* personal data, such as diagnostic data, telemetry, and logging, are usually not covered by these DPAs. And exactly these are the types of data that are relevant to the commercial purposes of the suppliers. So, when performing a DPIA, the university's focus should not only be on the processing of personal data by employees of the university in the course of their research or

[11] This can also be helpful in gaining a full insight in the data processing activities as input for the data processing register (article 30 GDPR).

educational activities, but on the processing of personal data that are generated from using the software as such.

5.2. Performing a Data Protection Impact Assessment

Performing a DPIA with a focus on the more technical types of data processing requires a combination of legal and technical expertise. A proven methodology is to make use of test accounts, write scenarios that represent common ways of working with the software, and then step-by-step execute these scenarios with the test accounts. At the time of execution, for every action a screenshot is made, and the data that are sent and received by the application are intercepted. After the tests, a data subject access request (DSAR) is filed to gain insight on transparency and processing purposes from the supplier by comparing the data received in reply to the DSAR with the intercepted data from the technical research. If necessary, the request is sent via the administrator of the organisation that is using the software. The supplier is a processor for the organisation (controller), and the DSAR has to be filed with the controller, who then asks the processor to provide the necessary information. The processor then has an obligation to cooperate and make sure that the controller can fulfil the request.

If all goes well, there is a clear and complete response to the DSAR within one month, or within six weeks if it is announced that responding to the request is complex and requires some more time. In these cases, the supplier provides a clear overview of the personal data processed about the data subjects connected to the test accounts. However, most of the time things run less smoothly and some extra effort is needed. For example, the input from the software supplier can be absent or incomplete. Or the supplier thinks that their response is complete by referring to the administrator for accessing the logfiles, and referring to the user (data subject) himself for direct access to the content data. Data that are generated and collected about the use of the software may not be included in the response.

Besides a DSAR, information about data processing can be obtained from logging. The logs can be available via the system administrator. Usually, there are two types of logging: application logging and transaction logging. Application logging is used to monitor the correct functioning of an application and includes logs on logins, logouts, and errors. Transaction logging is more detailed and contains logs on specific activities within the application. The level of detail of transaction logging can be modified by the administrator.

Finally, the supplier can simply be asked to provide other types of data they process, such as diagnostic data, including telemetry data and analytical data. These data are not always recognized as personal data and may therefore be excluded from the DSAR response. Based on the obligation to provide information to the data controller in the course of a DPIA, the supplier is held to cooperate with such a request. This falls under the general obligation to be transparent about the data processing so that the data controller can properly fulfil his information duties.

When data (from different sources) are received, an analysis can be made. First, this includes a technical analysis to verify whether the data provided are complete. This can be done by comparing the received data with the data that was intercepted during the test scenarios. If data are missing, the supplier can be asked to additionally provide these data or to explain why these data were not included. When data have not been provided and no valid reason was given, this may qualify as a lack of transparency and, thus, result in a risk in the DPIA. Next step in the technical analysis is to look for (pseudonymous) identifiers and determine what data can be related to specific actions from the test scenarios. Finally, it has to be determined what data qualify as personal data in light of the GDPR. For these data, a legal analysis must then be made on whether there is a legitimate ground for the processing thereof. An important part of this analysis is the verification of whether the processing of the data is mentioned in, and covered by, the privacy statement and in the agreements such as the Data Processing Addendum. The entire analysis will thus provide insight into the nature of the processed data, whether there are personal data, whether the processing activities are legitimate, and whether sufficient transparency is provided by the supplier.

5.3. Combining legal and technical expertise

High-quality legal and technical research makes it possible to gain clear insight in the data processing activities and the correct qualification of data from a legal perspective. This type of research requires sufficient time and resources and should be a robust process that allows for some back and forth. Performing such research allows for in-depth discussions between the university and the supplier on the factual processing of personal data by the supplier. By showing that there is a good understanding of the software and its workings, the customer-organisation encourages the supplier to also have the right people getting involved, i.e., those with technical knowledge about the workings of the software, instead of (only) the staff from the sales or legal department. Presenting the factual findings in a draft report further helps to open discussions about the exact processing of personal data. The supplier gets an opportunity to explain how and why certain data are processed. Moreover, the technical and legal experts working on the DPIA can demonstrate to the supplier how data are or can be connected to individuals and how datasets are combined. The discussions should first and foremost concern the facts, making sure that the findings as described in the report properly represent the factual data processing activities. Once the facts are agreed upon (or there is no convincing counter argument or evidence against certain findings), the qualification of the processed data can take place. This means that it is determined what data qualify as personal data and why. A common understanding on the facts and the data qualification helps to pinpoint where there may be any compliance issues .

There are certain risks that could arise from the lack of transparency when the supplier does not provide sufficient information about the processing, or when there is a discrepancy between the technical findings and the explanations, and the supplier's response to the DSAR. The risks that have been identified must be listed and appropriate mitigating measures should be defined. Not only the definition of the measure, but also clarity on the responsibilities for the measures and the timelines for implementing the measures have to be defined. When risks are not mitigated, it should be pointed out what the effects may be. A lack of transparency, for example, may hinder the data controller to adequately fulfil his information provision duties towards data subjects.

When high risks remain, the data controller can use the DPIA to ask the national data protection authority for a prior consultation. This is a serious instrument, since practice learns that the authority usually requires organisations to quit using the software and to take additional measures towards compliance. In the Netherlands, this was, for instance, the case with Google G Suite

Enterprise/WorkSpace.[12] With the data protection authority as a back-up, the data controller can create enough leverage from the DPIA to get the supplier moving.

As noted above, performing a DPIA requires specific expertise on the legal as well as on the technical level. Universities can share resources and expertise. However, there may be a lack of resources available, since a DPIA can be time-consuming and internal staff will have to do this next to their day-to-day tasks. And, there may be a lack of expertise or experience on specific aspects of the DPIA. Consulting external expertise may solve this problem. Experienced consultants will usually be better equipped to make a good estimate of the required time and effort, and what the best approach may be to perform a certain DPIA. Moreover, when the external consultants have a serious track record on DPIAs on large-scale software suppliers this will also help in the credibility towards the supplier and have the effect of getting access to the right information and contacts within the organisation of the software supplier.

Technical research can also detect international data transfers. If this is the case, a Data Transfer Impact Assessment is one of the measures to be taken to see whether this transfer does constitute high risks. Last but not least, a mandatory audit at regular intervals can help to stay in control and see whether there are no relevant changes in the processing activities on the high risk points of attention.

5.4. Power is in the crowd

Suppliers are not always willing to cooperate with an extensive DPIA. They have a power position and can simply force the acceptance of their products with their unilateral standard contract. A single business user, even when this is a university with maybe 2,000 employees using the software, is not that relevant for a supplier with millions of users worldwide. However, when scaling to a *sector*, it may become relevant. And when there is an opportunity to publish the DPIA, preferably in English, the outreach suddenly becomes much bigger and can cover the entire EU. A public document with findings on non-compliance with the GDPR can then have a serious impact, as it actually means that the use of the software is not allowed within the EU. On the other hand, when the supplier cooperates and there is an end result with a positive outcome, the supplier can benefit from this. So, "the power is in the crowd", or at least the ability to reach a crowd that is significantly large for the supplier.

A common practice is to create a so-called 'umbrella DPIA' that covers the data processing activities that are always taking place, regardless of the content that is produced with the software. In other words, an umbrella DPIA assesses both the data processing that is inherent to the use of the software application (such as logging, analytics, diagnostic data processing, telemetry) and the data processing activities that are laid down in the master business agreement and the data processing agreement and related documents. The umbrella DPIA can therefore be relevant for all universities

[12] See: https://slmmicrosoftrijk.nl/wp-content/uploads/2021/06/inzet_kantoorapplicaties_Google_G_Suite_Enterprise_door_de_minister_van_Justitie_en_Veiligheid_.pdf .

that use a certain software application. Based on the umbrella DPIA, universities can each make their smaller assessment depending on the way the software is implemented in their organisation and the specific data that are processed in that context. Collaboration also has the effect that repeated investments from different universities for the same research are prevented

Working together as a sector and being backed by a data protection authority when necessary is helpful when insisting on GDPR compliance towards suppliers. Negotiating contracts for the entire higher education and scientific research sector allows for better discussion and saves time and money as opposed to individual negotiations.

In the Netherlands, this way of working has proven to be successful. An example is the DPIA (and HRIA) performed on Facebook Pages as commissioned by the Dutch Ministry of the Interior and Kingdom Relations.[13] Or very recently the DPIA on AWS with amended contracts being negotiated for the entire Dutch government.[14] And earlier the Ministry of Justice, for instance, requested Privacy Company to perform a DPIA on Microsoft Office.[15] This 'umbrella DPIA' assessed the processing activities of personal data that always take place when using the software, without considering the specific data processing activities by an individual organisation in relation to their (public interest) tasks. The result was a DPIA with an overview of risks that apply more generally. The ministry negotiated the report to be published and to be written in English. The English language is both useful when discussing findings with international staff from the supplier, as well as for reaching a broader, international audience. Moreover, the results of the DPIA can be reused by other organisations to negotiate steps to bring a service or software to comply with the GDPR.

A comparable approach was taken by SURF and Sivon, two Dutch organisations representing the educational sector, with regard to the use of Google G-Suite for Education. In this case, the DPIA concluded that a number of high risks still remained. Since Google was not willing to make the necessary changes, a prior consultation at the Dutch Data Protection Authority was required. The result of that consultation was as expected: the high risks that had not been mitigated were deemed unacceptable, so the use of G-Suite had to be terminated. In order to not frustrate all kinds of educational programs too much, Google was given a limited timeframe to come up with mitigating measures. If Google would not succeed in providing a good plan and evidence, the use of G-Suite in the Netherlands would be prohibited. This was enough to convince Google and resulted in a remediation plan and serious changes in the contracts and some of the workings of G-Suite.[16] In this case, the developments were closely followed by an international audience. The results were taken up internationally by governments and supervisory authorities.

[13] See: https://www.privacycompany.eu/blogpost-en/dpia-on-government-use-of-facebook-pages-seven-high-data-protection-risks .

[14] https://www.privacycompany.eu/blogpost-en/new-dpia-and-dtia-on-aws-for-the-dutch-government-all-high-risks-solved .

[15] See: https://www.government.nl/documents/publications/2019/07/23/dpia-microsoft-office-365-online-and-mobile-slm-rijk-23-july .

[16] See: https://www.privacycompany.eu/blogpost-en/google-mitigates-8-high-privacy-risks-for-workspace-for-education .

Sector-wide collaboration could offer a way to share the resources and time needed to conduct meaningful DPIAs. When assessing a tool that is or will be used by more universities, the costs can be shared, as well as the time investments from employees that carry out the DPIA. One or two universities or university associations can take the lead and function as the point of contact towards the software supplier. The findings of the DPIA can be shared and reused within the sector.

The government can also support universities by collaborating on DPIAs and negotiations concerning software that is not only used by educational institutions but also by government institutions. Public policy can further help in setting priorities for the sector.

To conclude, DPIAs can be of help for universities that wish to (re)gain digital sovereignty. First, a DPIA helps a university in getting a clear insight in what personal data are processed when using a software application. This allows for taking decisions on the use of these applications and brings the necessary transparency to improve internal policies on the purposes for which the application may be used and what data may be processed, and what types of usage or types of personal data are not allowed to be processed by the software application.

Second, a DPIA forces the digital service supplier to cooperate and be transparent about how it processes personal data about the users of the software. This is helpful to minimise the information asymmetry and strengthens the position of the university.

And third, a DPIA is useful to collect evidence for data processing activities that are not compliant with the GDPR. This evidence can then be used to negotiate with the digital services supplier and to improve compliance and therefore the position of the university as a data controller.

6. Conclusion

Universities use many commercial software applications in the course of their academic research and teaching activities. As a result of interconnectivity between tools, and the availability of reliable functionality, universities have increasingly become dependent on (a few) large-scale software suppliers. Being too dependent on external suppliers can be a threat towards the independent position universities and academic researchers should have in society.

This memo described how the GDPR can be used as a means to improve digital sovereignty. Working on compliance with the GDPR, especially via the performance of DPIAs, helps in (re)gaining control over the data that are processed by software suppliers and the purposes for which the data are used. This approach has been successfully employed in the Netherlands vis-a-vis large U.S. based cloud providers such as Microsoft, Google and Amazon Web Services.[17] The DPIAs have proven successful as a means to:

- Increase transparency
- Limit unlawful processing activities by software suppliers
- Improve control over data for the customer
- Renegotiate contractual terms and conditions

With better agreements and good discussions on the scope of processing activities, universities can improve their position and become more digitally sovereign.

There are, however, limitations on what is possible, depending on available resources and time to perform high-quality DPIAs and the willingness to cooperate from the digital services suppliers. Nevertheless, the GDPR can be used as a strong and effective instrument to get software suppliers moving. A combination of high-quality legal and technical expertise is crucial to gather clear insight in the way software suppliers work and opens the way for negotiations on service improvements.

When universities have more control over the processing of personal data they can also better control the exercise of influence by the software supplier on users of the tools. Sector-wide collaboration enables universities to take a position with enough power to have a say in relationships with large- scale software suppliers. Ultimately, the GDPR can be used as an instrument to improve digital sovereignty of universities.

[17] See New York Times article: https://www.nytimes.com/2023/01/18/technology/dutch-school-privacy-google-microsoft-zoom.html .

PRIVACY COMPANY

In case of questions, please contact Arnold Roosendaal.

Arnold.roosendaal@privacycompany.nl

www.privacycompany.eu
info@privacycompany.nl
070 – 820 96 90

Maanweg 174
2516 AB Den Haag
14e verdieping

Postbus 95315
2509 CH Den Haag