Karen Felicia Hjertstedt Lansborg

INNAFOR

Developing an online self-help tool to ensure GDPR compliance in SMB´s

Master's thesis in Interaction Design
Supervisor: Frode Volden
June 2020

Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design

NTNU
Kunnskap for en bedre verden

Karen Felicia Hjertstedt Lansborg

INNAFOR

Developing an online self-help tool to ensure GDPR compliance in SMB´s

Master’s thesis in Interaction Design
Supervisor: Frode Volden
June 2020

Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design

NTNU
Norwegian University of
Science and Technology

CONTENTS

1 INTRODUCTION

1.1 ABSTRACT

Since the GDPR became law in May of 2018, larger corporations have been required to take measures immediately in order not to risk large fines for mishandling user data. Smaller companies have been given leeway and time to find their bearings with the fairly new regulation after voicing concerns about not having enough time to do what was required or learn about the subject. Now two years have gone by, and when doing a survey on the subject for this project several small businesses still stated that they do not know enough and are not ready. When looking online a small business owner would not find a quick and easy way to gain general knowledge about what is required specifically for their business. The tool developed in this project took aim to solve that by creating a free, easy to use and trustworthy tool that should help any small business get started on their compliance work.

By exploring the GDPR itself in great detail, the relevant articles pertaining to compliance in small business in particular were picked out, and they were boiled down to five key questions. These five questions ended up being the key component in the Innafor concept, forming the basis for creating an automated custom privacy policy to help small bisinesses. By answering the five questions truthfully, a general picture of how a small business handles user data in regards to the GDPR comes to light, and via an algorithm this is generated into a custom privacy policy - a must have for any company, big or small. From here it would be up to the small business to follow up on what is clearly stated in their custom generated privacy policy.

This tool was developed via codesign including small businesses themselves in the brainstorming and workshops required in the ideation and creation phase of this project. The design was further iterated by testing and retesting it on these small businesses themselves. Concluding this project is a plan to get the tool developed and released into the market during the fall of 2020.

1.2 KEYWORDS

GDPR | Compliance | PrivacyByDesign | SmallBusiness | DataPrivacy | CoDesign

1.3 RUTER - A STORY ABOUT GDPR COMPLIANCE

This is a story about how a large company with a huge standing in the nation's capital and a lot to lose, managed to not only become compliant, but set the gold standard for compliance. If they can do that, any small company should be able to at least comply, right? This story concludes with the interview subject coming up with an idea for a completely new angle to this project.

Talking about Big Data and Smart Solutions

While conducting an expert interview with a senior analyst at Ruter, a story about GDPR compliance done in the big league came to light. This semi-private public transportation company has done a remarkable piece of work to ensure they are not only GDPR compliant, but they set the golden standard. Until now, their two apps "Ruter Reise" and "Ruter Billett" have offered users travel options to get from A to B, and a ticket of choice that is both paid for and stored with data on your device. Going forward however, their two apps will be made into one, and the service will be made more personalized. There will for instance be an integration with Oslo Bysykkel and Oslo Taxi to give the users a more holistic experience of traveling in Oslo, having the Ruter app give suggestions to alternative travel options including these different means of transportation.

The technical aspect of how this will be done at Ruter was not discussed during this interview, but in short it involves using AI and gathering Big Data to understand user behaviour (Zhaohao Sun & Yanxia Huo, 2019) and integrating third party user data into the solution as well. This data will be stored in the cloud and be subject to the GDPR, the big question is whether there is a need for massive amounts of personal data to be able to make a personalized service like this, or if it is possible to do with data that is anonymous. Ruter is in the process of figuring that out, but first they will have to complete the testing of their new solution. The test phase is done in a closed group consisting of only 250 users, and the correct consent must be given by each and every person participating in the testing. The process of getting consent for this testing was what led Ruter into their rigorous work of becoming the best in class at GDPR compliance.

Getting to know the GDPR better within the company

When asked about the GDPR in general, the data analyst at Ruter said that breaking down what the GDPR is into parts that make specific rules is quite hard, what you do is figure out exactly what personal data you need to develop a service that will create value, and then make sure to handle only this small amount of data correctly. Whereas previous practices have been to gather as much as you can and figure out what you need later, there now needs to be a legitimate interest for all data collected and it needs to be collected at a minimum. Everything is tied to consent, users need to know exactly what their data is being used for, they need to be able to administrate and withdraw consent at any time, and there needs to be automated processes in place that deletes data once a consent has expired. All this is very time consuming and rigid, says the analyst, but it is definitely worth it.

> Figure out exactly what personal data you need to develop a service that will create value, and then make sure to handle only this small amount of data correctly.
>
> -Data analyst at Ruter

Once the GDPR came into effect, all employees at Ruter were given mandatory training. This consisted of training given by the compliance manager at Ruter and a legal firm specializing in the subject. Employees were divided into small groups that were given training both in person and via an e-learning platform. The topics were fairly general, but also tied into what Ruter employees might need in their projects.

> No one expects us to be experts, but it is important to have enough knowledge about the GDPR to identify when it is relevant to think about it. Knowing when to pull in the experts is very useful, rather than continuing on ahead blindly. Having enough knowledge to be able to do this right creates great value.
>
> -Data analyst at Ruter

Knowledge about the GDPR did exist prior to it being put in effect, but several years ago nobody knew what would happen or what "personal data" was really pertaining to, and there was talk of huge fines that could potentially bankrupt any company that did not comply. Now we know that this is not the case, says the data analyst, Datatilsynet does not ride around like executioners looking for companies to finish off. Fair warning is always given, and they will provide help and assistance when needed.

Developing the Diamond Standard

Heading into a rather large testing phase of a new Ruter service, a red flag was raised by the spouse of a test user. This person happened to be an expert on the subject of GDPR and raised a concern about a consent being requested retroactively, where it needed to have been gathered ahead of the gathering og data. This was a fairly small issue, but Ruter took it very seriously regarding it as a potential symptom of larger issues. The whole project was halted, and a rigorous six month process began.

Firstly, an investigation was started at Ruter, beginning with a full DPIA risk analysis (datatilsynet.no, 2019) on the entire technical solution. A special task force was established at Ruter, and their first task was to contact Datatilsynet to inform them about the issue; contacting them will have to be done within 72 hours of discovering a potential breach (datatilsynet.no, 2018). Six months of the task force developing new routines resulted in all consent being gathered prior to gathering any data. This consent is given digitally, but also on paper in case of the digital systems failing. Should that happen, any work on the project would have to stop completely, but having these consents in paper form provides an added security. All consents given have an expiration date and are not valid beyond this date.

The changes that have been the most noticeable in the day to day work in this project has been the change of third party services. Previous providers such as Slack (slack.com) and Survey Monkey (surveymonkey.com) both store data in the cloud and are not particularly preoccupied with GDPR compliance as they are based outside of the EU. Therefore Slack has been replaced with a lesser, but GDPR compliant chat software called Rocket Chat (rocket.chat) that is run locally. All surveys are now done with Questback (questback.com), a Norwegian based company that takes GDPR very seriously. They even have a template that lets you create ready-to-go surveys that you can be sure are within the regulation’s parameters.

The privacy policy for this test project was developed by Ruter in collaboration with several official bodies and the details were specifically formulated down to the last detail. The final policy became eight pages long and the information is presented in a way that is easily understandable for anyone. Each section is tied to the consent it pertains to, and there is a table of contents for easy access to any section. Terms of service may change when there is a bug fix or change to the service. Updates and bug fixes are done in bulk so the user of the service will not have to consent to changes in terms of service too often. Many people might get annoyed with the little cookies and consent box popping up, but we are in a time where asking this question is very important and people simply need to get used to being asked, says the data analyst.

Thoughts on what might be a useful tool

A useful thing would be to have a summary for a project telling you "These Are The GDPR Issues You Need To Be Concerned About In Your Project" so you would not have to think about all potential threats at once. That would be nice, but it is hard to get a “one size fits all” issue summary for projects that could collect a wide variety of data in large projects owned by big companies where it is difficult to keep track of who is collecting what. If one were to ignore the difficulty of doing this on a large scale, it would be ideal to have some form of automated service where one could enter what type of service or project that is being developed, says the analyst, and then get a generated GDPR compliant template or a list of things to look out for in that particular project.

1.4 FINDING THE RIGHT QUESTION TO ASK

Why change the initial research question?

The initial plan for this master project was to find out what GDPR compliance needs service designers doing large projects have. The goal was to gain insight into which part of Smart Services result in privacy-issues and why, underlining the hypothesis that doing large scale, innovating projects while respecting the GDPR poses a challenge for service designers. Early on in the research process however, the initial research question proved not to be a viable one.

> What kind of GDPR compliance issues hinder scale up of large Smart Services innovation today, which measures are being taken to work with or around the issue of collecting Big Data, and what kind of tool will be an effective, easy-to-use privacy-aid for service designers in their daily design process?

Based on a survey (Appendix 1) done among digital designers working in large companies and municipalities, findings (Appendix 2) showed that there is little need for an easy-to-use GDPR compliance tool in large scale projects. Most of the answers showed that Privacy by Design is already a part of the workflow in large companies, and that they have the tools at hand to help them comply with the GDPR. Only a very few responses showed a lack of knowledge or an ignorant attitude. Presented as a sample in a petri dish (Fig. 1) the problematic areas shown in darker shades make out a much smaller part of the results than anticipated. So much so, that changing the entire research question became the only logical course of action.

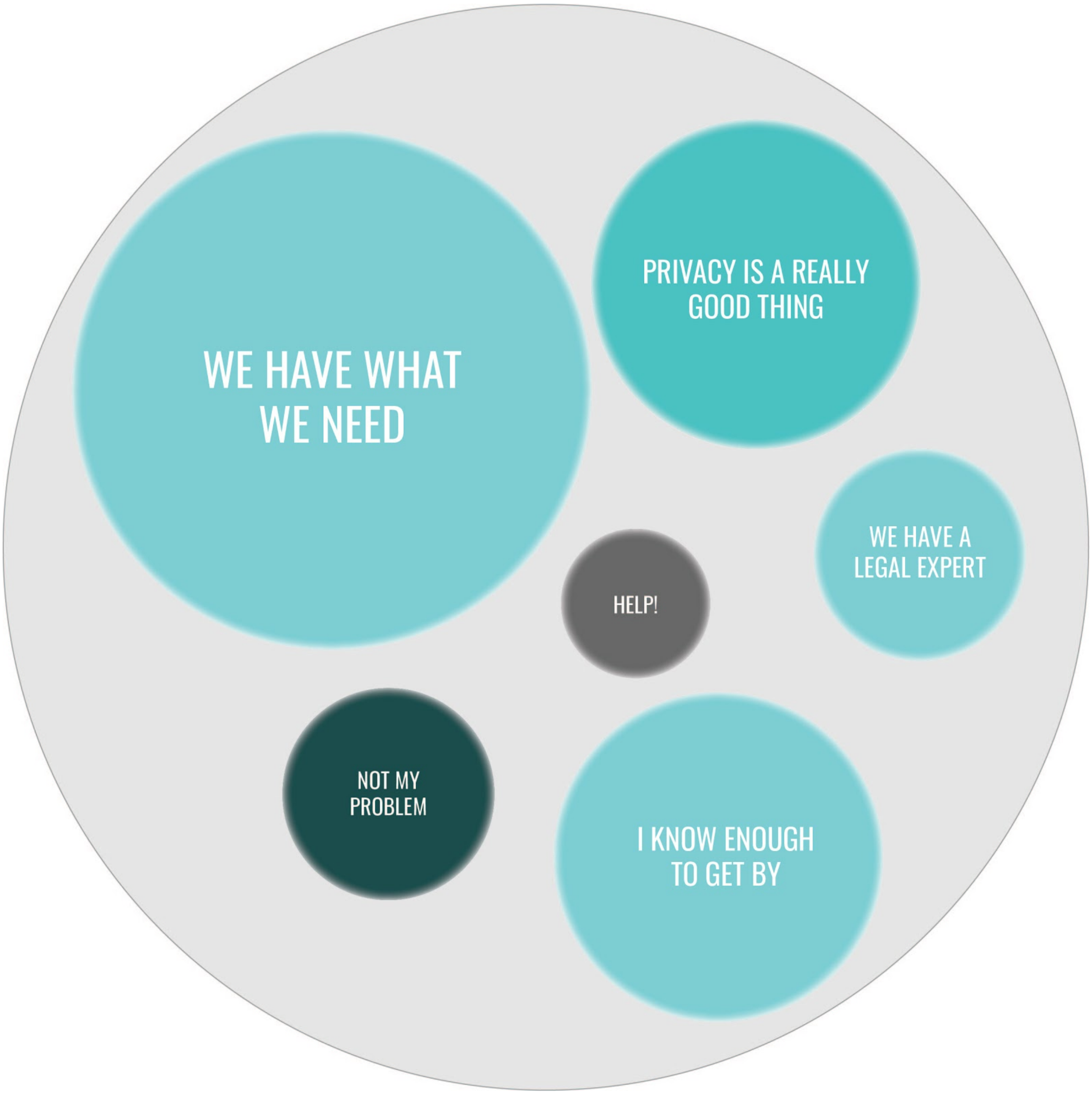


Fig 1: Results from a survey done among service designers (5) in large companies.

When talking off the record to fellow interaction designers, many pointed out that although large companies might mostly have the tools they need, small businesses consisting of one or two employees are often left alone. The GDPR does not affect them as much due to the fact that small digital design companies and their limited amount of clients presumably do not handle large amounts of data and so not as much emphasis has been put on what impact the GDPR has on them because they are not the big threats to privacy of everyday people, that would be the larger corporations. However, a survey done by GDPR.eu done in May of last year shows that there is great ignorance among small businesses owners, and the report emphasizes that this is very problematic due to the fact that small businesses would most likely not be able to afford a large GDPR fine (gdpr.eu, 2019).

In 2016 25% of Norwegians worked in small businesses with 20 employees or less (nho.no, 2020). According to Forbes online in 2019 Norway was one of the most exciting countries to watch out for when it came to startups (Forbes.com, 2018). These small companies often consist of only one or two people having an idea and running with it. Should they succeed and scale up to begin production and sales where the gathering of user data is required, they are going to need GDPR-knowledge. If only two people work in a company and their main business has nothing to do with privacy laws, the likelihood of this being in focus is very low. Becoming aware of this, shifting the focus of this project to be about small business compliance became the logical choice. Before getting into the project, a story about GDPR compliance in a large organisation will provide context and insight about what goes into proper compliance work.

1.5 RESEARCH QUESTION

Here is the research question for this project:

Will an easy-to-use GDPR compliance tool made available for free help small businesses implement privacy in the development of their services? Will this tool make them more compliant than they were without it, and will having privacy as a feature in their service also create value for their business?

2 METHODS

2.1 RESEARCH METHODS

Literature research

This project drew upon findings from the Specialisation subject done in preparation for this thesis to create general context about “Privacy by design” and “GDPR”, adding more literature pertaining to the new subject of GDPR compliance in small businesses in particular. Regarding the specifics of the GDPR itself, the original regulation text was used as a source. The developed tool created in this project was built on a solid foundation of knowledge about the GDPR itself, combined with an understanding about the potential user group’s needs.

Survey methods

Two surveys were conducted for this project, the first of which was done as part of the Specialisation subject mentioned above. This was a large survey done to map out general attitudes in the public, and so it was distributed anonymously among family and friends with no specific target demographic.

The second survey targeted service designers, and in order to get a reasonable sample size the scope was widened to include anyone doing digital design in larger companies. The questions for this survey were open ended so the answers could be used to get an idea of attitudes and notice key phrases. Results of this survey were presented in the very beginning of this paper and will not be a part of the further work, as the findings only served to show that the project was not viable with this user group.

Interview methods

In the planning of this project, interviews were to be the main source of qualitative data. Due to time constrictions, interviews on potential end users were done in written form online. This allowed for easier distribution, however the answers given were much shorter than had the interview been done in person with the possibility of asking participants to elaborate. A consideration was made to whether having short answers was better than no answers at all, and the answer was yes; having insights about attitudes and knowledge among small businesses would prove useful even if the answers were minimalistic. These participants were the main user group for the tool being developed, understanding their needs was a key component to success.

A possibility to conduct one hour long interviews in person became available, and even though the person interviewed had been deemed outside the scope of this project because they work for a large company, the interview was conducted to give a better understanding of GDPR-compliance from a practical standpoint. The work of the interview subject did overlap with the new target user group in several places, and so the relevance of doing an expert interview with an analyst in a big company was considered relevant and was thus included in the beginning of this thesis to give context and general insight into the subject of GDPR compliance.

Ethical considerations

Both surveys were conducted with Google Forms (Wikipedia: Google Forms, 2020) This is not considered a GDPR compliant tool due to Google's questionable handling of user data resulting in one of the largest GDPR fines to date (cnil.fr, 2019) and another fine as late as march of this year (datainspektionen.se, 2020) but since all data gathered was anonymous, this tool was considered to not pose any real threat to the privacy of the interview subjects. The first survey did not include any open ended questions that could include sensitive or identifying information by accident, however the second survey consisted of only open ended questions. While going through the answers, none of the answers contained any identifying or sensitive information and so they were all kept.

Online interviews were mostly conducted via Google Forms as well. These were also done anonymously, and like the second survey all questions were open ended, increasing the chance of accidental gathering of personal data. When going through the data, no such identifying or sensitive data was found and so all the responses were kept. The one expert interview conducted in person was taped and written consent

(Appendix 3) was given beforehand, stating that the interview was anonymous and that its contents would only be used for the purposes of this project, and that the recorded interview will be deleted at the end of this project on May 31st 2020.

2.3 DESIGN METHODS

Design workshop method

One workshop was held in this project. It was hosted at a neutral location with sufficient space and atmosphere to conduct a productive session of co-design. In the workshop several game storming methods were used such as Affinity Mapping (Gray, 2010), Brainwriting (Stickdorn, 2018, p. 180), Crazy 8s (Gilbert 2016), Dot Voting, and a Graphic Jam (Gray, 2010). The plan was to have a two hour workshop, including an opening mingle session with soup. Expected attendance was between three and five participants, hand picked for their competence in the field of digital design.

Technical design method

To keep the momentum from the workshop, the design sketches were developed into an digital interactive prototype within a few days (Stickdorn 2018, p. 236) and remained fairly true to form from. In this phase the digital mock up of the tool would showcase ideas for graphic communication and layout from the workshop as well as basic functionality. Once the final feedback from the workshop participants was given, a final design was made using wireframing in Marvel (marvelapp.com).

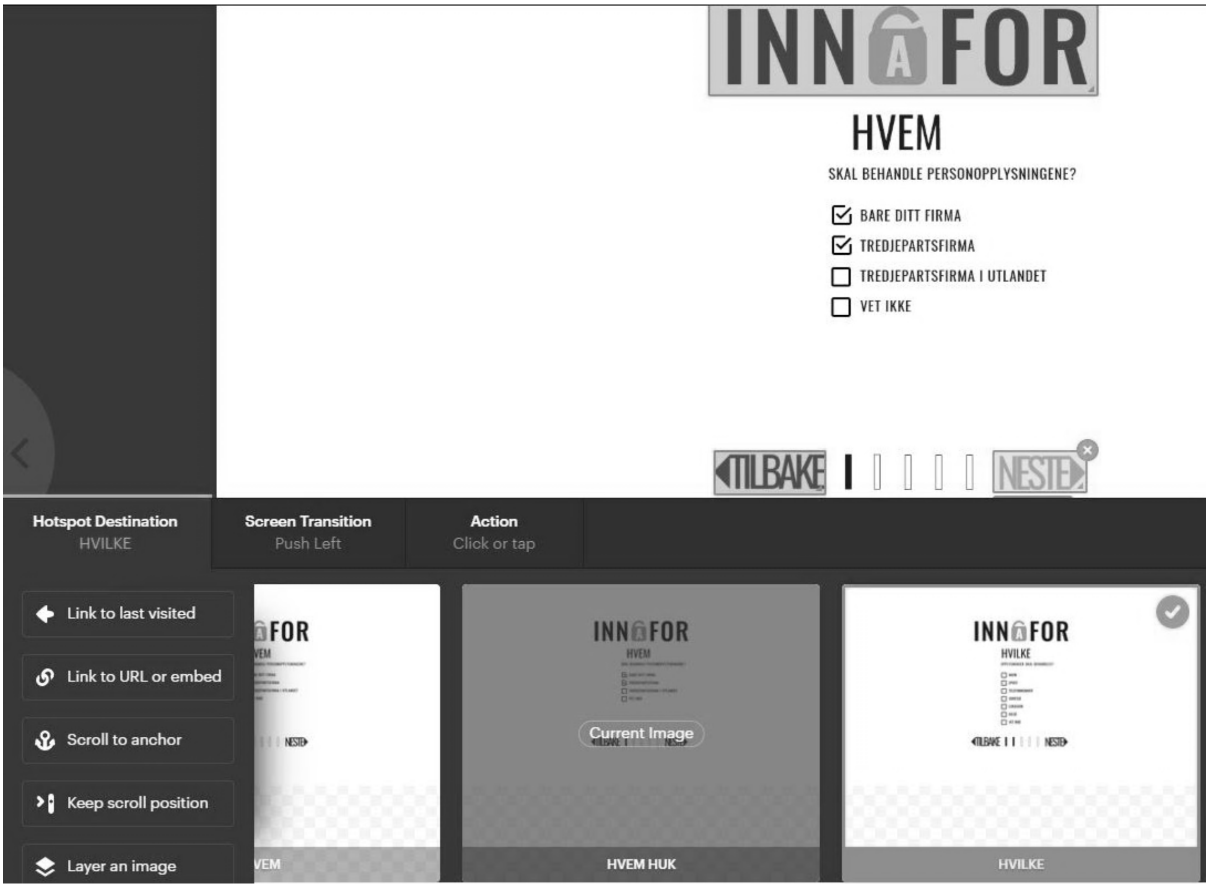
The functionality of the tool was never built by a developer, but the information architecture was designed and the final prototype wireframe included all the copy needed to make it into a finished tool: A website with GDPR information and check boxes describing different levels of data handling, which the small business could fill out to match their own data handling process, resulting in the output of a tailor made privacy policy text ready to use for their particular service. The boxes in the wireframe prototype were pre-checked for a mock company, the test users themselves could not actually fill out any of this freely as the tool was only a high fidelity prototype, but it gave them a general idea of the functionality.

2.4 TESTING METHODS

Testing method phase 1 - Digital interactive prototype and survey

Apart from the workshop, most interviews and research was done remotely online, and this was the main method of testing for the remainder of the project due to social distancing caused by the global pandemic (who.int, 2020). Not being allowed to gather more than five people at a time outdoors prevents any testing in person (fhi.no, 2020) In order to test the prototype remotely online, the testable prototype needed to be very easy to understand. Using Marvel this was easy to achieve. This tool allows you to use still images of your design and make parts of it clickable. Each clickable part links to another site, which is also simply an image with clickable parts leading on to another clickable image etc. Once the prototype is finished, one can create a link to it, and then send this link to test subjects.

The results from the workshop would first have to be made into a digital design in order to be tested, this was achieved by making a wireframe. The wireframe for the Innafor prototype was made in Adobe Xd and consists of simple free design icons from a plugin and original designs made in Adobe Illustrator. To make this into a clickable prototype in Marvel, a screenshot of every possible frame of the site was taken from the wireframe and then uploaded to Marvel. Once uploaded, the pictures were linked together by highlighting the different buttons on the site and making them clickable (Fig 2). This included making certain button clicks result in error messages. The prototype was not a functioning website, it was all an illusion giving an impression of the visual design and function of the website or app, that is all.



INNAFOR

HVEM

SKAL BEHANDLE PERSONOPPLYSNINGENE?

☑ BARE DITT FIRMA
☑ TREDJEPARTSFIRMA
□ TREDJEPARTSFIRMA I UTLANDET
□ VET IKKE

Hotspot Destination: HVILKE
Screen Transition: Push Left
Action: Click or tap

Fig 2: Making a digital interactive prototype in Marvel

When distributing the test, the test user received an email with a link to the Marvel prototype and another link to a Google Form survey to give feedback, with instructions to simply click through the prototype and then fill out the survey. This was all anonymous, and the test user was informed of this (Appendix 4). The survey consisted of closed questions to establish to what degree the test users were in the target demographic for the Innafor tool, and open ended questions to give feedback on the tool. They were asked to give feedback both about the visual design and the overall function and idea of the tool. Doing both at the same time saved time for the project. The initial testing was done on a prototype that was in its very early stages to get as much feedback as possible on all the things that did not work as they should or looked horrible. This in a way made the testers a part of the design team, continuing with the co-design principles used in the workshop.

Testing method phase 2 – New prototype and survey about purpose

The second testing phase technically worked the same way as the first one, except the prototype was more or less finished visually, and the test focused more on whether the function of the tool serves its purpose, which is to help small businesses and organisations cope confidently with the GDPR. The prototype in this second test phase was tested in the user testing functionality of Adobe XD, which is a much better tool than Marvel once you know how to use it (there was a learning curve during this project). To distribute the test, a second email went out with two links, one to the finished prototype and one to a Google Forms survey, but the text in the email emphasized that this was a test focusing on whether the tool is helpful or not. The information architecture and content of the tool was much more finished and detailed than the first prototype. The goal of the second test phase was to answer the research question for this thesis; will an easy-to-use GDPR compliance tool made available for free help small businesses implement privacy in the development of their services? Will this tool make them more compliant that they were without it, and will having privacy as a feature in their service also create value for their business?

3 LITERATURE RESEARCH

3.1 WHAT IS THE GDPR?

The GDPR explained

To make this tool hit the target user group, finding the information in the GDPR that is relevant for them is key. The point of this tool is to help small businesses comply in the areas they are affected, without them having to read through the entire GDPR to understand which parts they are. Therefore, a big part of preparing to make this tool was reading and understanding the GDPR, and then picking the sections that would be relevant for a small business. They might not gather much data or use it on a large scale like bigger companies, but there are still areas to look out for.

The General Data Protection Regulation of 2016 states that:

> *"Controllers of personal data must put in place appropriate technical and organisational measures to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate), and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit, informed consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation, or unless the data controller or processor has received an unambiguous and individualized affirmation of consent from the data subject. The data subject has the right to revoke this consent at any time."*

(Wikipedia: General Data Protection Regulation, 2019)

This is the GDPR's purpose. The regulation consists of 11 chapters that have all together 99 articles (gdpr-info.eu, 2018).

The 11 chapters in the GDPR are:

Chapter 1 (Art. 1 – 4) General provisions

Chapter 2 (Art. 5 – 11) Principles

Chapter 3 (Art. 12 – 23) Rights of the data subject

Chapter 4 (Art. 24 – 43) Controller and processor

Chapter 5 (Art. 44 – 50) Transfers of personal d to 3rd countries or international organisations

Chapter 6 (Art. 51 – 59) Independent supervisory authorities

Chapter 7 (Art. 60 – 76) Cooperation and consistency

Chapter 8 (Art. 77 – 84) Remedies, liability and penalties

Chapter 9 (Art. 85 – 91) Provisions relating to specific processing situations

Chapter 10 (Art. 92 – 93) Delegated acts and implementing acts

Chapter 11 (Art. 94 - 99) Final provisions

When reading the 99 articles in the GDPR, only sixteen of them are directly relevant to the method used for the amount of data gathering done by small businesses with limited need for such data. These articles have been extracted from this text and are instead listed and explained in Appendix 5. They will be referred to later as they play an intricate part in the design.

3.2 WHAT IS REQUIRED OF A NORWEGIAN BUSINESS

The Norwegian parliament decided to implement the GDPR into the EØS agreement to make it valid in Norway the same as it is in the EU. In Norway it came into effect July 20th 2018, and it is Datatilsynet who enforces this law (gdprdokumentasjon.no, 2018). Following is a list of all things smaller Norwegian businesses are obligated to do in order to be compliant according to Datatilsynet.

Protocol for data processing activity

The data controller is required to have a log of the data being processed in the form of a protocol. Any third party who handles the data should also have a protocol about how they handle the data. There is a template for this protocol at the Datatilsynet website (datatilsynet, 2018). This protocol is essentially a list of the type of data the business intends to collect, and it is to be written in Microsoft Word, Excel or OneNote. Once this protocol is in place it makes it easy to retrieve data if a data subject asks to look at the personal data stored about them or if Datatilsynet pays a visit (bedrebedrift.no).

Privacy by design

As mentioned earlier in this paper, the seven principles that make up Privacy by Design, are at the heart of the GDPR. The seven principles are meant to guide anyone who is responsible for developing or maintaining the systems, technical or administrative, surrounding the handling of personal information (datatilssynet.no, 2018).

Internal control

Just as there are internal documents describing how to handle terms of employment and the economy of a business, there needs to be routines surrounding the handling of personal data. An internal control consists of three elements that will help ensure the correct handling of data: The governing elements, which are rules and protocols for the leaders of a company to develop and follow up, the implemented elements, which are the actual rules the employees have to follow, and the controlling elements, which should be run routinely to catch breeches (datatilsynet.no, 2018)

Determine purposes for data gathering

A business needs to determine what the data being gathered is intended for. This is in order to not gather more data than necessary, and also to be able to get informed consent from a data subject. They need to know what their data is being used for in order to consent. The third reason the purpose should be determined before gathering any data, is because the nature of the data gathered determines how long it can legally be stored. Once a purpose is determined and communicated to data subjects whose data is being collected, this purpose cannot change without informing the data subjects of this

Establish a valid basis for the handling of data (samtykke)

In order to gather any data, the business also needs to have consent and a good reason to gather the data. For a small business, these reasons could be needing email addresses to send out vital information or relevant information, or a payment method and address to get paid for a product and then send it to the correct address. THese reasons vary and should be considered on a case to case basis. Only the relevant data should be gathered, and should only be stored during the time it is being used (datatilsynet, 2019).

Be prepared to handle users exercising their rights

If a user i.e. wants to know what is stored about them or wants to have their data changed because of errors, this should be done for free and as quickly as possible. Before doing so, the business needs to verify the person's identity, so as to not be an unwilling participant in fraud. The business (data controller) should be prepared to be able to do this if the need should arise (datatilsynet.no, 2018).

Data protection officer

If a business is largen than approximately 40 employees, there should be a designated data protection officer who is responsible for giving advise about how the business and its employees should handle personal data and issues surrounding this (datatilsynet.no, 2018). DPO should have general knowledge beyond the basics and be able to assist on a case to case basis. In many bigger companies, the DPO has legal background so as to better understand the legal terms in the GDPR. For smaller businesses, this point is not really relevant.

Data processor agreement (made by the the data controller)

Any business, big or small, who shares personal data about their customers with a third party, a data processor, is obligated to have a data processor agreement (databehandleravtale). This agreement is made by the data controller, in this case the small, and and is in place to ensure that any handling of the data by the third party is compliant with the GDPR and operating within the same specific limitations as the data controller (datatilsynet.no, 2018). This is relevant altso for a smaller business, because they might not realize that they are using a third party data processor when they i.e. use Google Suit to handle documents and emails, or Survey Monkey to do customer satisfaction surveys, but they are and there needs to be an agreement in place in order for the small business to be able to inform their customers of what data is being handled, by whom, how, and why (bedrebedrift.no, 2018).

Transferring personal data out of the country

This point has a low probability of being relevant, but if a small business has say two employees working in Thailand or a colleague located in London for a time being, there are things to consider. In short, transferral of data can happen unproblematically if the receiving country has what is deemed to be sufficient privacy laws of their own, so transferring data within the EU would not require any extra action. If however the data is transferred to Thailand, a country with lacking privacy laws, then special agreements would have to be in place ensuring the compliance of standard privacy regulations established by the European convention (datatilsynet.no, 2018).

When and how to inform Datatilsynet about a breech

When there has been a possible breach, the business has 72 hour to report the breach to Datatilsynet. According to them, a possible breach could be if personal data has been sent out to the wrong person, if personal information about other people than the recipient is included in a correspondence, visible personal data on the outside of packages sent by mail, mail that has been opened before arrival at its destination, cases where hacking could have resulted in data theft, employees going through colleagues personal info without good reason, authentication and password protection is not secure and could result in people who should not have access gaining access to the personal information of others, information being published without being anonymized, a break in where computers or paper documentation includes sensitive information, discarding old data without destroying it or anonymizing it, or loosing a document or file . All these things should be reported within 72 hours of it happening, especially if it could lead to discrimination, theft of identity, fraud, economical losses, loss of reputation or life. The report that is sent should include the nature of the breach, the number and type of people it might affect, some parts of society are more vulnerable than others. It should also include what types of personal data have possibly been mishandled, possible consequences of the breach, and what measures have been taken to rectify the breach and its consequences. If all of this is too much to handle within the 72 hour time limit, one can send a preliminary report and add more information at a later date, but as soon as possible. (Jarbekk, 2019, p. 273-277)

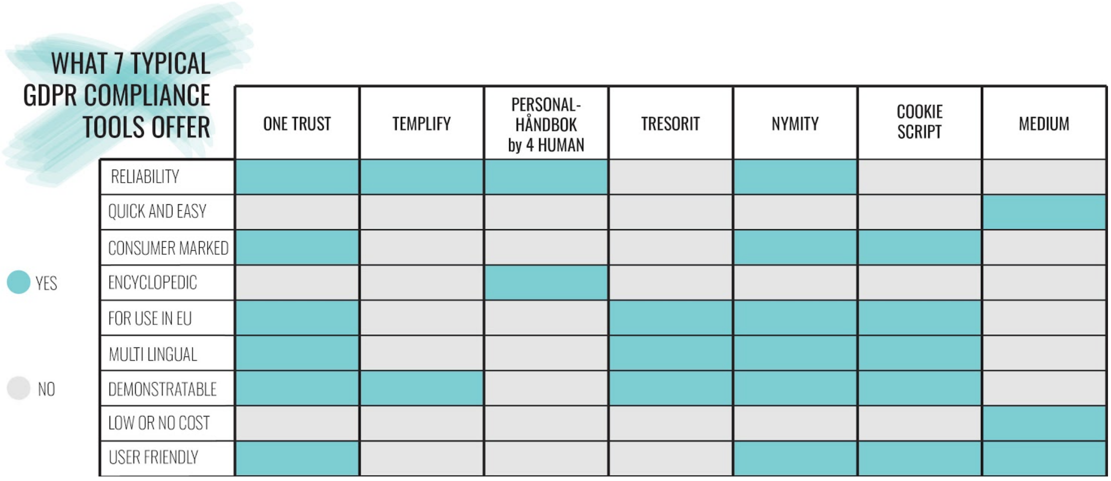
3.3 SMALL BUSINESS GDPR ISSUES AND TOOLS

There are third party tools available today that help a business keep the collection and storage of personal data inside the law, but the top tools showing up in a simple Google search for “GDPR compliance tools” are huge and complex tools made for corporations dealing with massive amounts of both old and new data. These tools are understandably expensive, but paying for this level of complexity is often out of the question for a small business only gathering small amounts of data like e.g emails and subscription data. The criteria for the tool being developed in this project were that it should be easy to use, free (for initial use), quick, trustworthy, for use in the EU (not the US) and preferably in Norwegian. The tools that showed up on a simple Google search did not fit these criteria, neither did tools made specifically for the Norwegian market, or even the ones made for smaller businesses. This will be explained shortly.

Examples of existing GDPR tools and how they work for SME's

Protecting user privacy can be looked at as a chore but when presented in a certain light, protecting people's personal data can be highlighted as a feature, thus creating great value for a company. Even with a positive attitude like this, the meere scope of the GDPR is so wide that although Ruter had the opportunity to develop their own tools for compliance, the resources needed to do so are not available for small businesses. When comparing the top seven Google search results for "GDPR compliance tools" to see if any of them would offer a free, trustable, easy to use GDPR compliance assistance, the results showed that although the different tools met some of the criteria this project aims to meet, none covered them all.

The tools compared were OneTrust, Templify, Personalhåndbok by 4 Human, Tresorit, Nymity, Cookie script and Medium. These tools were picked because they represent the top choice in several different categories of tools. OneTrust is a large and complex tool specializing in easy to use data handling assistance for large amounts of data, while Templify is a template tool within Microsoft Office often used by larger companies with the need for control the format of documents across an organisation. Personalhåndbok by 4 Human is a type of GDPR encyclopedia, which is not at all like Tresorit which is a safe cloud storage, or Nymity which is an expert tool for compliance managers to develop demonstrable privacy programs for larger companies. Cookie script is mostly for front-end developers wanting to secure their code, they are not technically designers, but in a small business they might wear many hats. Medium is not a technical tool at all, but when doing a Google search about GDPR for small businesses, several Medium blog posts by expert show up, and so it is logical to include it as a possible source of information The criteria behind the tool being developed are seen in the column to the right in Fig 3. Tools that show up in a Google search fill some of these, but none of them do all of what this tool is meant to.



WHAT 7 TYPICAL GDPR COMPLIANCE TOOLS OFFER

● YES

○ NO

	ONE TRUST	TEMPLIFY	PERSONAL-HÅNDBOK by 4 HUMAN	TRESORIT	NYMITY	COOKIE SCRIPT	MEDIUM
RELIABILITY	●	●	●	○	●	○	○
QUICK AND EASY	○	○	○	○	○	○	●
CONSUMER MARKED	●	○	○	○	●	●	○
ENCYCLOPEDIC	○	○	●	○	○	○	○
FOR USE IN EU	●	○	○	●	●	●	○
MULTI LINGUAL	●	○	○	●	●	●	○
DEMONSTRATABLE	●	●	○	●	●	●	○
LOW OR NO COST	○	○	○	○	○	○	●
USER FRIENDLY	●	○	○	○	●	●	●

Fig 3: Seven tools and what they offer

Examples of tools made specifically for small businesses in Norway

Datavernarkivet (datavernarkivet.no) is a tool that do all the things the tool developed in this project is meant to do, but it does a number of other things and is rather comprehensive, and it also costs NOK 590 per month in a subscription fee. If a small company does find that they do store a substantial amount of data and the simple tool developed in this project does not address all the issues faced, Datavernarkivet would be a good next level tool to use. They cover:

- Register for consents given
- Privacy Statement generator
- Newsletter Privacy Statement generator
- E-Commerce Privacy Statement generator
- Templates for presentation
- Record of activities
- Knowledgebase
- Record of inquiries
- Privacy center
- Privacy evidence
- Register of breaches

Bedrebedift.no is a site that quite thoroughly goes through what small businesses need to think about to comply with the GDPR. This site has a series of articles describing different areas where even a small business needs to take extra care about how information is handled, and how to do it. These articles are well written and very informative, and a great place to start to get a general idea of what the GDPR means to a small busines. The site altso makes privacy policy templates with video tutorials, this has a fee og NOK 990. In addition, the site offers personal training and assistance via phone to get started, this leads to receiving a protocol and tailored privacy policy. The cost of this is NOK 6900. Before receiving this help, the site requires you complete their mini training on GDPR online, which is free. For NOK 9900 a small business can receive the basic training, plus assistance in dealing with specific types of data, a risk assessment and an overall quality check of their entire site (bedrebedrift.no, 2020).

4 INTERVIEW AND SURVEY RESULTS

4.1 USER ATTITUDES TOWARDS GDPR

When users are suspicious about a website's intent, it is important that the communication of intent is very clear. 68% of participants in the survey described in this section said they trust websites and online services, they would not look out for errors or contact the website if something was confusing or questionable. This makes it all the more important that the responsible party lives up to that trust and handles personal data correctly, otherwise a visit from i.e. Datatilsynet could end up with them being fined and even worse, the personal data of their customers or clients being misused.

In the survey done at NTNU last year in preparation for this thesis (Lansborg, 2019) 50 participants in a survey were asked what they knew about the GDPR and how it affects them. 74% of the participants were between the ages of 31 and 50, and occupations were fairly evenly distributed between technical and non technical occupations. When asked if they knew what the GDPR is, 90% answered yes. When asked to choose from a variety of suggestions explaining what the GDPR means to them as an end user, 86% of them answered that the GDPR is in place to ensure that websites and online services ask permission before handling their personal data (Fig 6). This answer proved that a sizable number of people in the target demographic of working adults do indeed understand what the GDPR means for them.

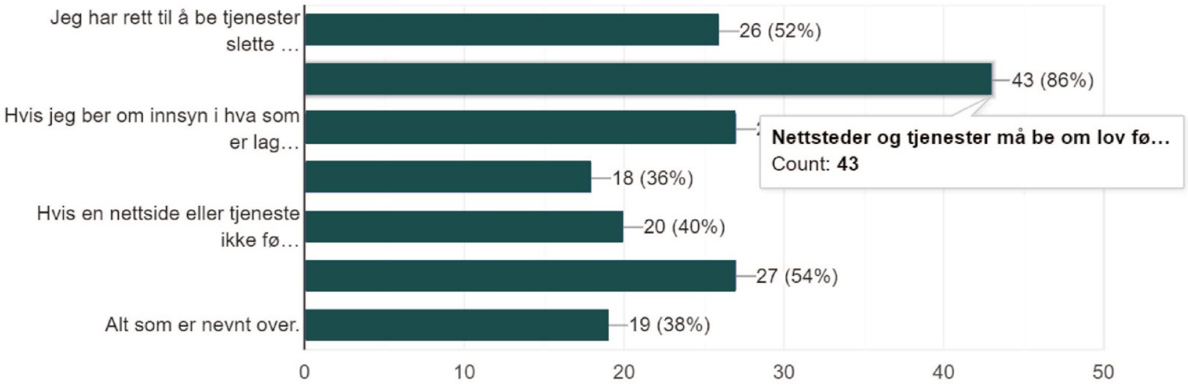


Fig 4: Survey results showing user knowledge about what the GDPR is meant to do.

When asked specifically what they do when prompted with an end user agreement asking them to click "OK", 44% answered that they click "OK" without reading because they trust the website, and 24% read the terms of the agreement, and then always agree to them after reading. 20% of the answers showed the attitude of people being annoyed with these prompts, while as much as 20% (14% + 6%) said they get suspicious or wonder what they are trying to fool them into when these boxes pop up (Fig 5).

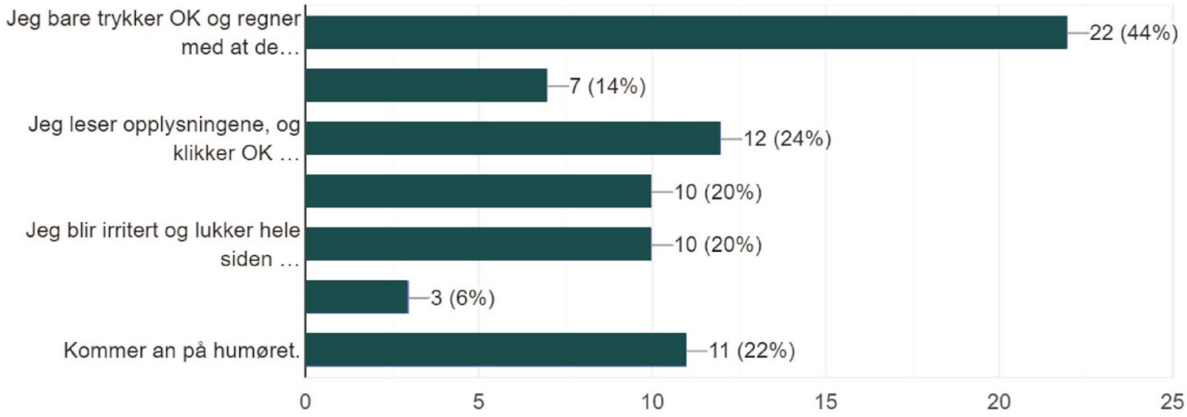


Fig 5: Survey Results about user attitudes towards GDPR and digital user privacy.

4.2 SMALL BUSINESS ATTITUDES VS THE MEDIA

To test the theory that there is a need for an easy to use, ready available free tool to help small businesses comply with the GDPR, a combination of online interviews and searches in online news articles was done to gather data. Finding small businesses that would answer even just a few short answers proved to be difficult. To gather a general idea of what small businesses might struggle with, an email was sent to smb.no (små og mellomstore bedrifter) with a few short questions about what they experience as most challenging among the small businesses that come to them for help. (Appendix 6) Another two participants representing small businesses were also asked to answer the same questions via email. As for the media's point of view, a Norwegian Google search for "GDPR småbedrifter" gave a result of a whole search result page full of articles. Going through the articles, E24 had the angle of highlighting the challenges of compliance in two separate articles (e24.no, 2018) were written by law experts on the subject and are intended for an expert audience (the newspapers in question are not tabloid). The information was therefore deemed as a valid source on the general attitudes toward GDPR from a trustworthy media source.

The next step in finding out whether the hypothesis of the need for a quick and easy compliance tool for free is indeed watertight, was to do word count on relevant words and phrases throughout the articles and answers from the interviews. Relevant words and phrases were: challenges, costs, worry about getting it right, whether learning and understanding the subject is hard, attitude towards protecting personal data in general, willingness to learn and improve on the subject, and the perceived availability of GDPR tools that are easy to use and not too expensive. Going through the three interviews and the three articles, part of the goal was to compare the statements of small businesses with what the media claims are the issues. This is to better understand where there are assumptions in the media or bias in a small business owner's narrow point of view, and where there might be an overlap indicating a real need. Results of this comparison word count are shown in Fig 6.

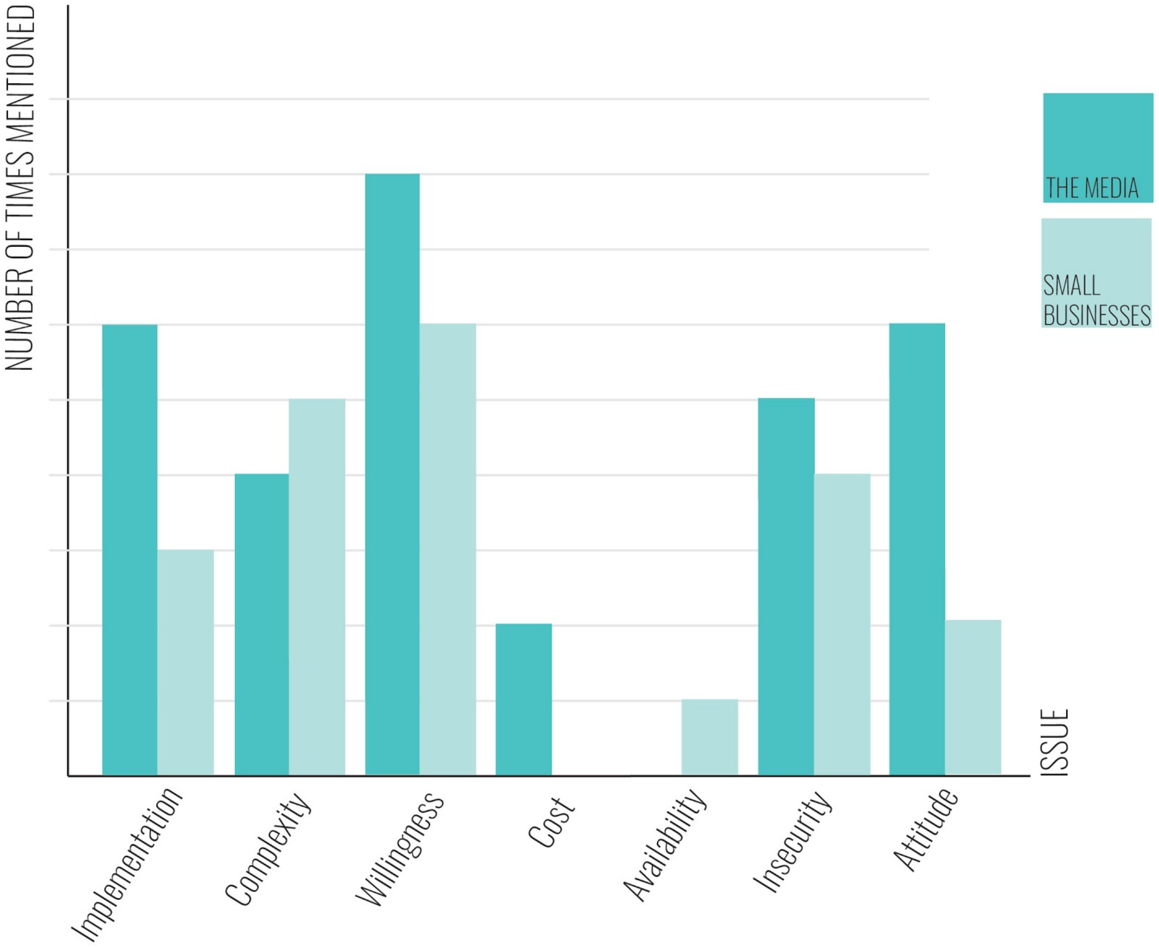


Fig 6: Keywords and key phrases from small businesses compared to the media.

4.3 KEYWORDS AND PHRASES COMPARISON

Implementation

As in any business, there is an established way of working in a small business. There might be a certain case handling routine that involves several steps, or a file system that is organized in a certain way in a manner that suits the responsible persons way of thinking. This has been acceptable for a long time, but now the GDPR is requiring secure and proper handling of data and information, which might require a business to redesign their entire system for handling information. In the interviews and news articles, issues surrounding this were mentioned six times by the media, while the small businesses themselves only mentioned it three times. In other words, experts in the area seem to think that this is going to be an issue and thus it most likely will be at some point, but small business owners do not realize they likely have to restructure the way they work and they might be surprised down the line.

Complexity

Learning about the GDPR and understanding what measures are necessary, if any, is a part of what a small business will have to do to comply. Both the media and the businesses themselves agreed that this is a concern, because the subject matter is so complex that it may lead to misunderstandings and consequently errors in the handling of personal data. Even if the intent was good, errors may occur, leading to fines. For now, Datatilsynet are fairly lenient on a case to case basis (hence the Ruter collaboration experience), because of the complexity of the subject.

Willingness

There seemed to be a willingness to improve and comply with the GDPR among the small businesses, and the news articles also reflect this. Despite this work requiring several non-billable hours, businesses seemed to realize that having the protection of personal data as a priority is required to keep credibility in any market.

Cost

The cost of implementing tools and resources to help with compliance was not mentioned once by the businesses themselves, and only once in the news articles. Looking at available tools online they all have a fairly high monthly cost for a company of only two or three employees, and this leads to the theory that cost should be an issue, but this was not the case according to this exercise. However, operating under the assumption that any business aims to keep expenses at a minimum, cost will still be a factor in the tool made for this thesis.

Availability

Finding information about the GDPR easily is important if small businesses are to be able to help themselves. In the news articles, this was not mentioned. In the interviews, it was only mentioned once. Neither the experts or the small businesses themselves seemed too worried about accessibility of information. This might mean that the GDPR being available online is deemed enough. The information is available, no doubt, although it may be hard to understand in its raw regulation form.

Insecurity

This is the point that might be the most interesting one for this thesis. Small business and the experts cited in the news articles agree that insecurity about whether sufficient and correct measures are being taken to comply with the regulation is a large concern. This concern is at the heart of what the tool made in this project is trying to remedy, which is making sure small businesses have what they need to confidently handle the personal data of their customers and users. This is also what Ruter hinted at in their interview; where they are a large company that are able to fund large projects devoted to compliance in order to make sure everything is in order, smaller businesses do not have the luxury of doing this.

Attitude

The focus on the big picture regarding data protection being a positive factor in all our personal lives was understandably more in focus in the media news article than with a small business owner. The results of this exercise show this clearly, as it was only mentioned twice by the businesses and a total of six times in the news articles. Thinking about all the good things that could come from being vigilant about protecting everybody's personal information is a meaningful exercise that could lead to a greater understanding of why all the fuss is about, but it might not be at the front and center of what a small business owner thinks about when threatened with heavy fines.

5 DESIGNING AND PROTOTYPING

5.1 CODESIGN WORKSHOP RESULTS

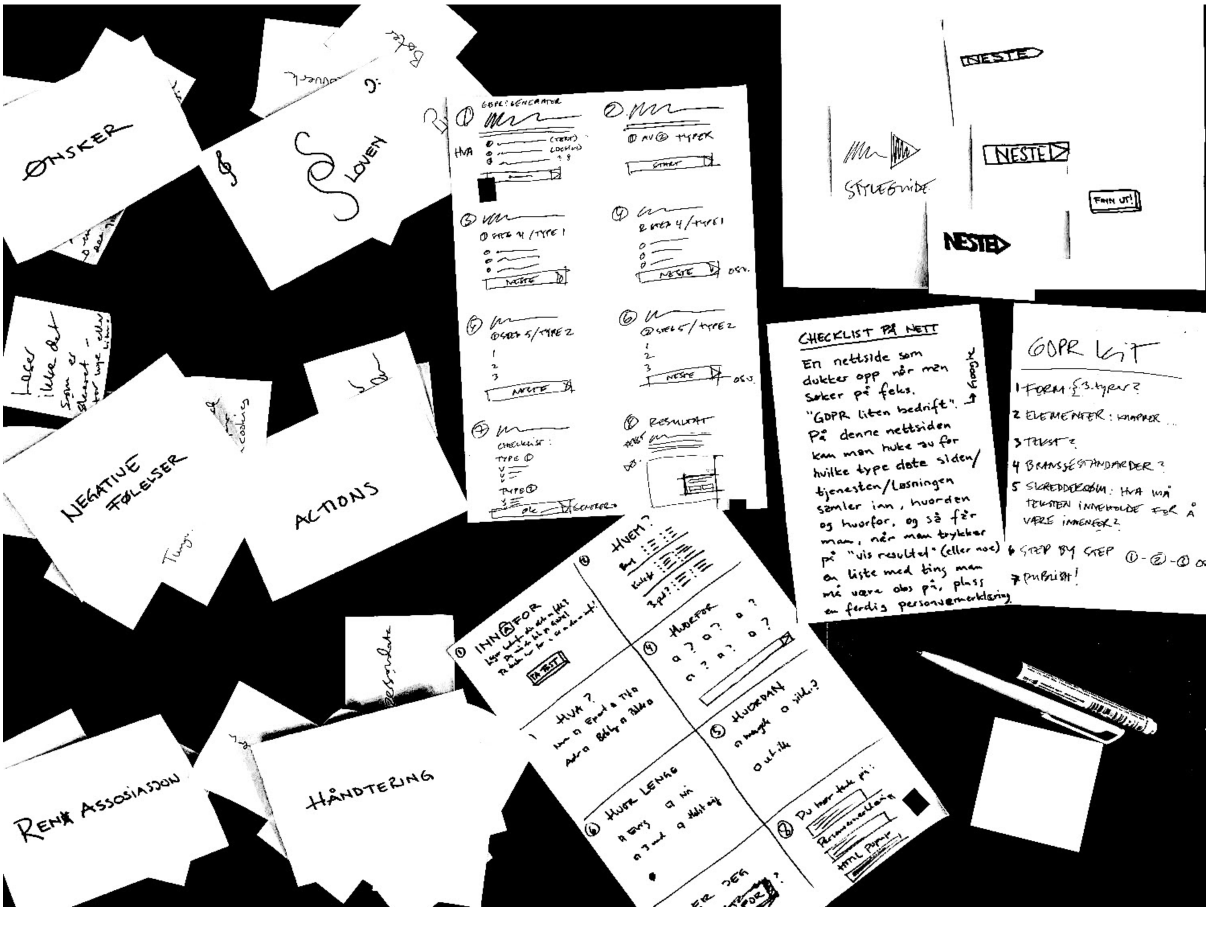

ØNSKER
LOVEN
NEGATIVE FØLELSER
ACTIONS
RENT ASSOSIASJON
HÅNDTERING
GDPR: GENERATOR
HVA
NESTE
RESULTAT
CHECKLIST
TYPE ①
TYPE ②
INN FOR
TA TEST
HVA ?
HVEM ?
HVORFOR
HVORDAN
HVOR LENGE
STYLEGUIDE
NESTE
NESTE
FINN UT!
CHECKLIST PÅ NETT
En nettside som dukker opp når man søker på feks. "GDPR liten bedrift". På denne nettsiden kan man huke av for hvilke type data siden/tjenesten/løsningen samler inn, hvorden og hvorfor, og så får man, når man trykker på "vis resultat" (eller noe) en liste med ting man må være obs på, pluss en ferdig personvernerklæring
Google
GDPR KIT
1 FORM {3 typer?
2 ELEMENTER: KNAPPER ...
3 TEKST ?
4 BRANSJESTANDARDER ?
5 SKREDDERSØM: HVA MÅ TEKSTEN INNEHOLDE FOR Å VÆRE INNENFOR?
6 STEP BY STEP ①-②-③ OSV
7 PUBLISH!

Fig 7: *Results of participatory design workshop.*

To start the design process, having someone from a small business participate in the initial flow of ideas was crucial. Just like Privacy by Design requires data privacy be a part of a design from start to finish, participatory design, or co-design, sees the value of including the end user of a system or site in the design process from the very beginning. We might be the designers, they are the experts on what they need (slideshare.net, 2016) In the workshop for this project only two people showed up, both studying and working in the field of digital design. Details about their background or identities are not relevant for this project, and will not be shared. Despite the low attendance, there was still time for soup and all the workshop games described earlier were also completed, ending with the results in Fig 9. Here, thoughts and associations surrounding the GDPR were sorted into categories that were then named. The six categories ended up being handling of data, pure associations, negative feelings, actions, the law, and wishes. With this in mind, and knowing this tool was meant to be a website and not a mobile app, loose thoughts were written down in a list describing what this tool might look like and how it would work. This was done on a timer so as to not overthink it. Once done, there was a discussion and decision on which idea to go with, and whether to implement elements from other suggestions; one idea did not exclude the other. The idea of having small businesses fill in a number of checkboxes to map out how they handle personal data was agreed on, and after drawing ideas out on paper, the idea of dividing it into categories of who will handle the data, what is being gathered, why, for how long and how is it stored. These are the very basic things any business has to think about when it comes to handling personal data under the GDPR, and so presenting the question in this logical order was considered a logical aid in helping users understand what this is all about.

A general look and logic of this tool was agreed upon, and the final exercise was to draw out the design quickly and then compare designs. This was perhaps the most interesting exercise; even though the general look was to be the same, when drawing it out two quite different results emerged. The two most noticeable differences were the placement of elements on the site and the navigation. Some button design and icon sketching was also done to finish up the workshop, and the “next” button and progress bar ended up looking quite unique (Fig 9).

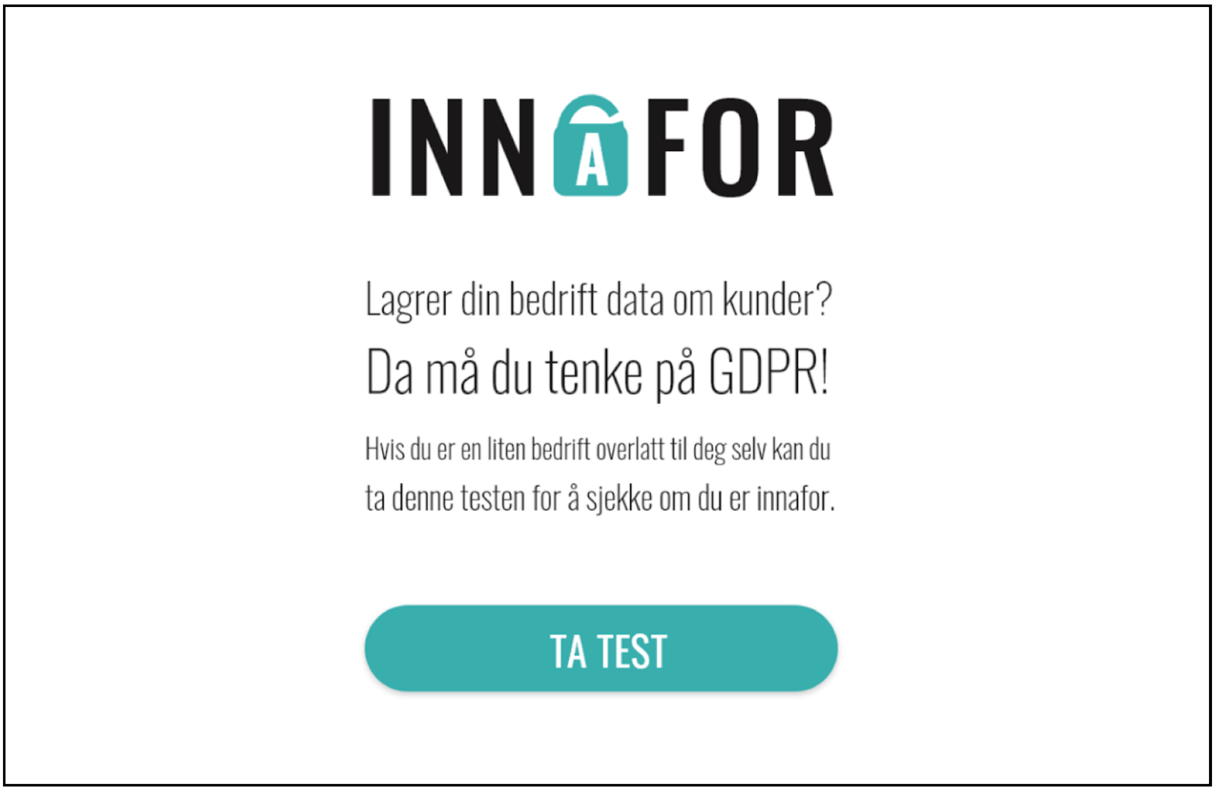
5.2 PROTOTYPE WIREFRAME RESULT

The final result of the workshop design was an seventeen page wireframe sitemap containing a front page (1), five pages with questions (2-6) with a corresponding identical answer page with checked boxes (7-11), an error page (12), and five versions of a result page viewing different states of scrolling in the text box (13-17). This was all screenshotted and put into the Marvel prototype testing tool and linked together by making the different buttons in the design lead to the correct destination page, as explained in the methods. Once the prototype was built, the link to it was distributed to six test users.

5.3 TEST PHASE 1 - THE PROTOTYPE

The first test was done as part of the design phase, a way of continuing the participatory design from the workshop. Going into the first test phase, this prototype was purposely less than perfect. The obvious mistakes in the design were there to get feedback on what could be an ideal solution for a final version. The theory (proven correct) was that instead of testing several good options, testing one bad one might lead the test users to suggest other options on their own. In this test, users were gathered by asking colleagues and friends, and them asking their colleagues, bosses and friends, the so-called snowball method (statisticshowto.com, 2014). All the users either are working or have worked in small businesses after 2018 (when the GDPR came in effect) and come from a designer or business background.

Starting at the beginning, the first page of Innafor is designed on a narrow grid, giving the feel of navigating through an app, despite being in a browser (Fig 8).



Lagrer din bedrift data om kunder?

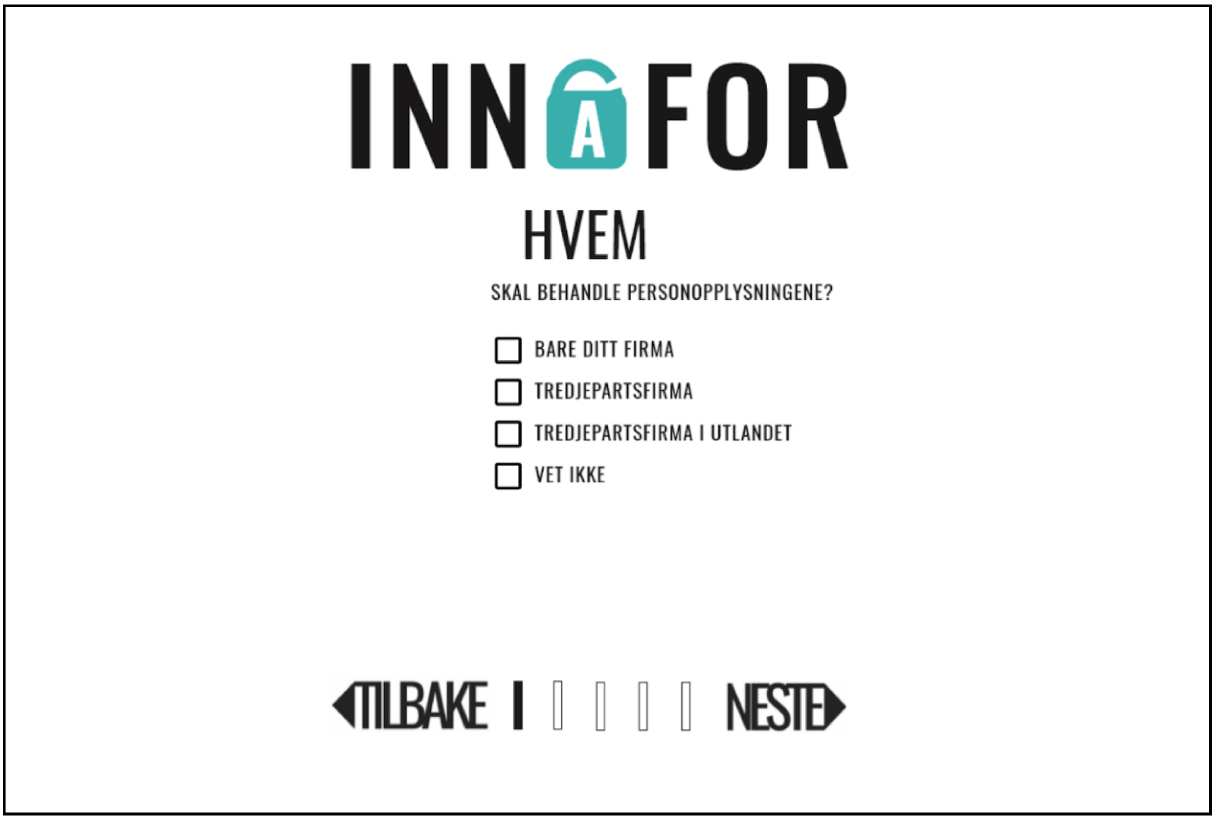
Da må du tenke på GDPR!

Hvis du er en liten bedrift overlatt til deg selv kan du ta denne testen for å sjekke om du er innafor.

Fig 8: Early prototype first page.

This narrow grid was chosen as a work around to avoid having to make the prototype responsive for mobile, this design fits on most screens except a phone.. When testing, results showed that this choice led to several comments (Appendix 7 – Test results phase 1) and an overall reference to the tool as "an app", which it never was and will never be. The different font sizes on the first page were also overall a bad design choice in hindsight, and there were comments on this from the testing as well.

The check box part of the tool was designed in the same narrow grid as the first page, also with unorthodox stylistic choices in typography and the placement of elements, emphasizing the key questions of who (hvem), what (hvilke), why (hvorfor), how long (hvor lenge) and how (hvordan). This part of the design did not receive much feedback, except for one user complaining that the progress bar was unclear. It was made in the co-design workshop and deemed a finished feature, but it had to be revisited.



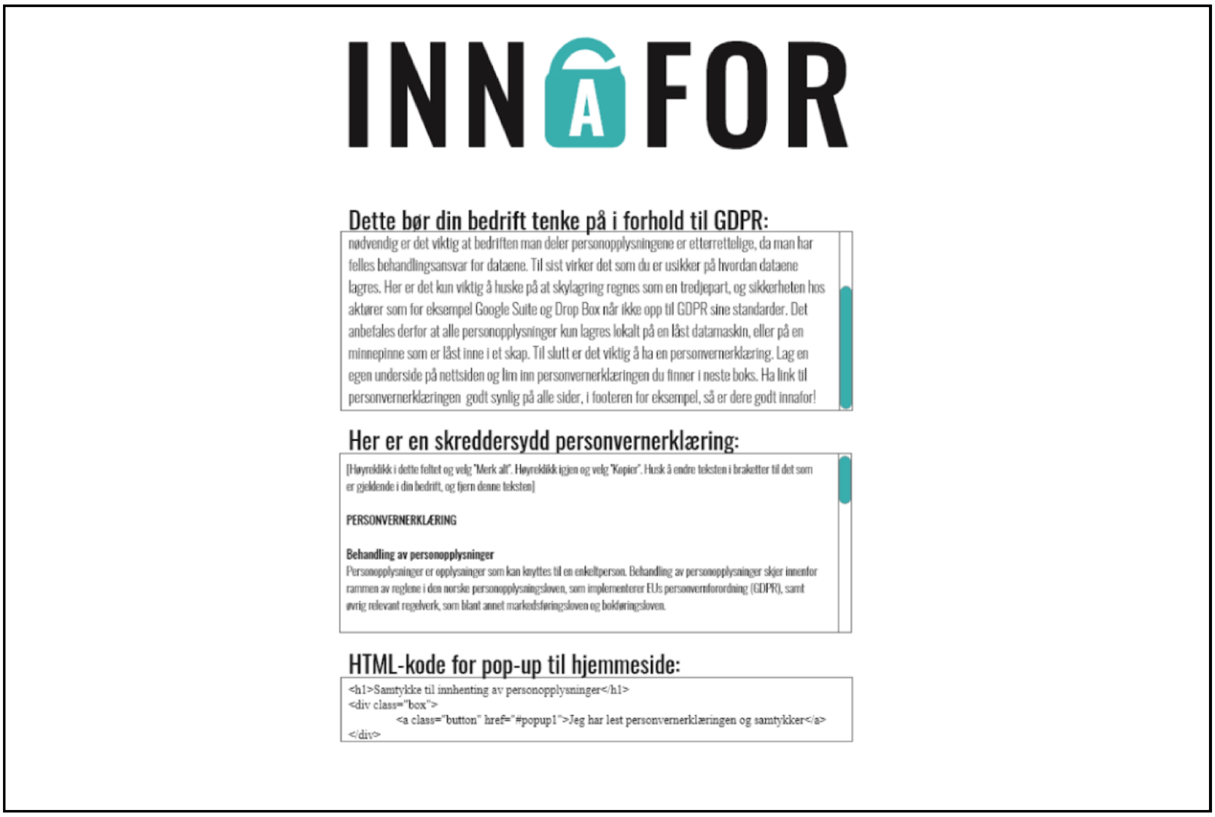
HVEM

SKAL BEHANDLE PERSONOPPLYSNINGENE?

- □ BARE DITT FIRMA
- □ TREDJEPARTSFIRMA
- □ TREDJEPARTSFIRMA I UTLANDET
- □ VET IKKE

Fig 9: Early prototype checkbox page

At the end, one obvious flaw in the initial design was the display of the final results. The tips for the small business and the privacy policy meant to be copied out was barely readable, and was contained in a scrollable box within the narrow grid. Every user commenting on this said this was a major design flaw. So much so that the questions surrounding the usefulness of the tools were almost ignored due to the fact that it was not possible to read the results of the test.



INNÅFOR

Dette bør din bedrift tenke på i forhold til GDPR:

nødvendig er det viktig at bedriften man deler personopplysningene er etterrettelige, da man har felles behandlingsansvar for dataene. Til sist virker det som du er usikker på hvordan dataene lagres. Her er det kun viktig å huske på at skylagring regnes som en tredjepart, og sikkerheten hos aktører som for eksempel Google Suite og Drop Box når ikke opp til GDPR sine standarder. Det anbefales derfor at alle personopplysninger kun lagres lokalt på en låst datamaskin, eller på en minnepinne som er låst inne i et skap. Til slutt er det viktig å ha en personvernerklæring. Lag en egen underside på nettsiden og lim inn personvernerklæringen du finner i neste boks. Ha link til personvernerklæringen godt synlig på alle sider, i footeren for eksempel, så er dere godt innafor!

Her er en skreddersydd personvernerklæring:

[Høyreklikk i dette feltet og velg "Merk alt". Høyreklikk igjen og velg "Kopier". Husk å endre teksten i braketter til det som er gjeldende i din bedrift, og fjern denne teksten]

PERSONVERNERKLÆRING

Behandling av personopplysninger
Personopplysninger er opplysninger som kan knyttes til en enkeltperson. Behandling av personopplysninger skjer innenfor rammen av reglene i den norske personopplysningsloven, som implementerer EUs personvernforordning (GDPR), samt øvrig relevant regelverk, som blant annet markedsføringsloven og bokføringsloven.

HTML-kode for pop-up til hjemmeside:

```
<h1>Samtykke til innhenting av personopplysninger</h1>
<div class="box">
        <a class="button" href="#popup1">Jeg har lest personvernerklæringen og samtykker</a>
</div>
```

Fig 10: *Early prototype final result page (unreadable text).*

In addition to the paragraph font being unreadable, the overall readability of the tool was also commented on several times as being bad. The placement of the text was shifted around and both the headings and the form text was in all caps lock, which simply does not look good according to the users.. Overall, the problem areas to emerge from phase 1 of testing are shown in Fig 11 and in more detail in Appendix 7 - Test results Phase 1.

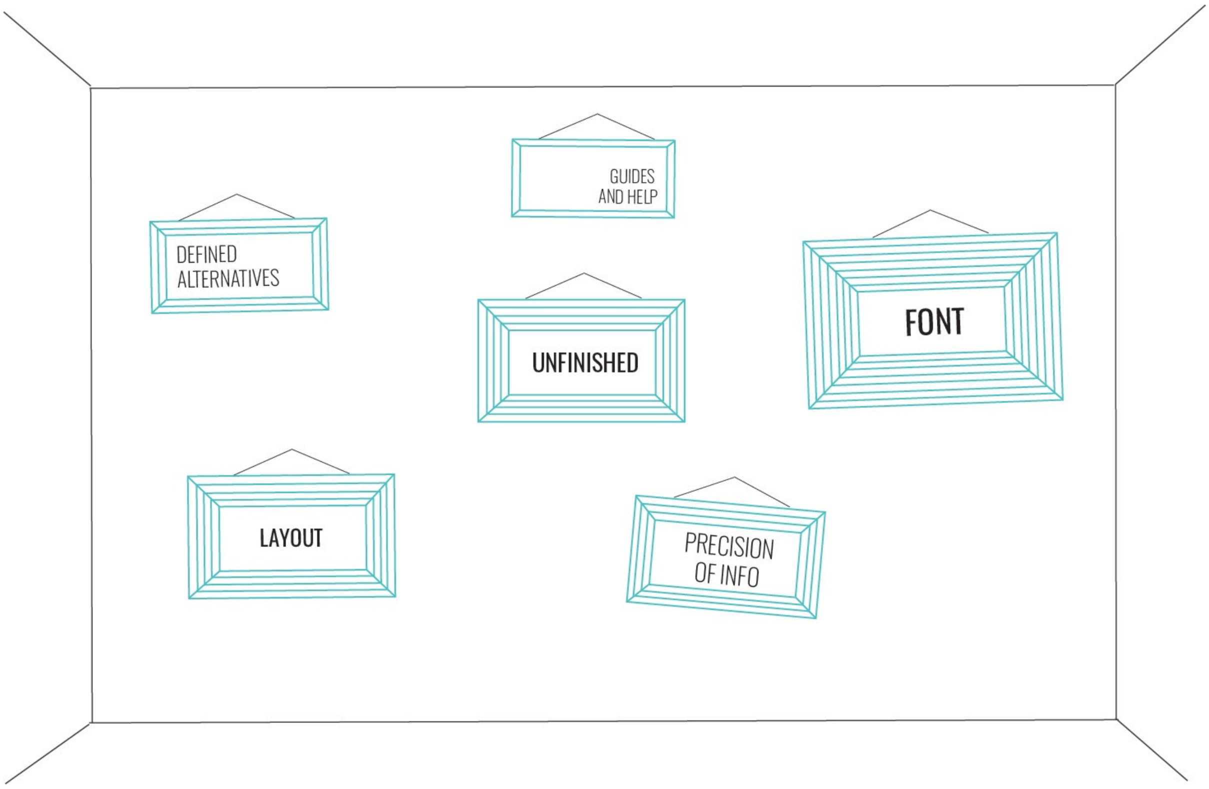
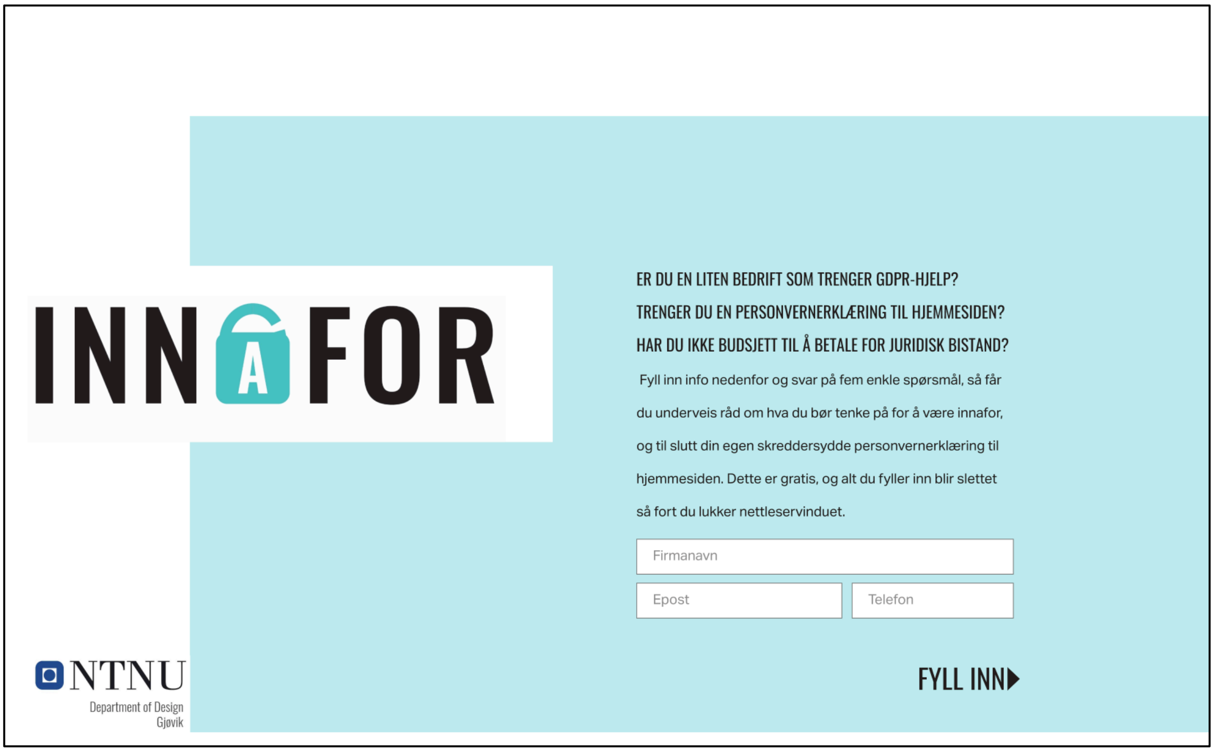


Fig 11: *Testing phase 1 results - problem areas arranged by frame size.*

6 FINAL DESIGN

6.1 THE FINAL FRONT PAGE

The first page for Innafor ended up looking quite different from what it did in test phase 1. There was a comment about all the different font sizes on the first page, which was made that way as a design feature for recognizability. That was a bad design choice, a bright idea that turned out not to be so bright. The new front page is a full width page, that also includes a tiny form asking for an email, a phone number and a company name. This is to better tailor the final privacy policy at the last page, more about this in the next section. There is a bit more information on the front page about what this site does, as well as a logo from NTNU which should serve as a stamp of quality (Fig 12). The entire final prototype is in Appendix 8.



ER DU EN LITEN BEDRIFT SOM TRENGER GDPR-HJELP?

TRENGER DU EN PERSONVERNERKLÆRING TIL HJEMMESIDEN?

HAR DU IKKE BUDSJETT TIL Å BETALE FOR JURIDISK BISTAND?

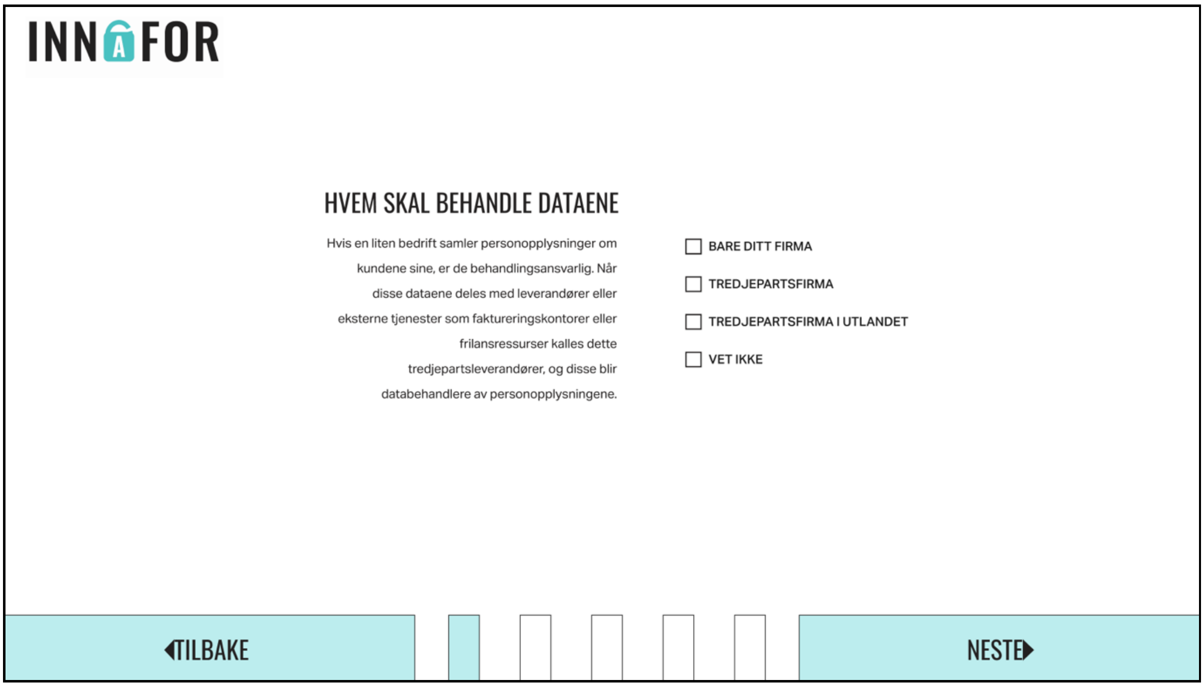
Fyll inn info nedenfor og svar på fem enkle spørsmål, så får du underveis råd om hva du bør tenke på for å være innafor, og til slutt din egen skreddersydde personvernerklæring til hjemmesiden. Dette er gratis, og alt du fyller inn blir slettet så fort du lukker nettleservinduet.

Fig 12: Final version of first page for Innafor.

6.2 THE FINAL CHECKBOX PAGES

For the checkbox pages, a user mentioned that it was difficult knowing what to choose, and so having the informative part of this tool (tips and tricks) on each checkbox site explaining how they might be relevant became the new solution. This is also in keeping with what is called UX-writing, a way of having carefully crafted copy be a part of the interface design to enhance the user experience (uxplanet.org, 2017). Having the communication with the user be spread across the entire site left the final page to be only the privacy policy, since the HTML code also ended up being excluded (more about that in a moment). The information listed here is all based on the relevant chapters handpicked from the GDPR (Appendix 5).

The navigation on the site was also mentioned, one user commented that the buttons did not look like buttons, and so they were designed to look more like conventional square buttons, with a matching progression bar that was also a bit bigger than in the first version (Fig 13).



HVEM SKAL BEHANDLE DATAENE

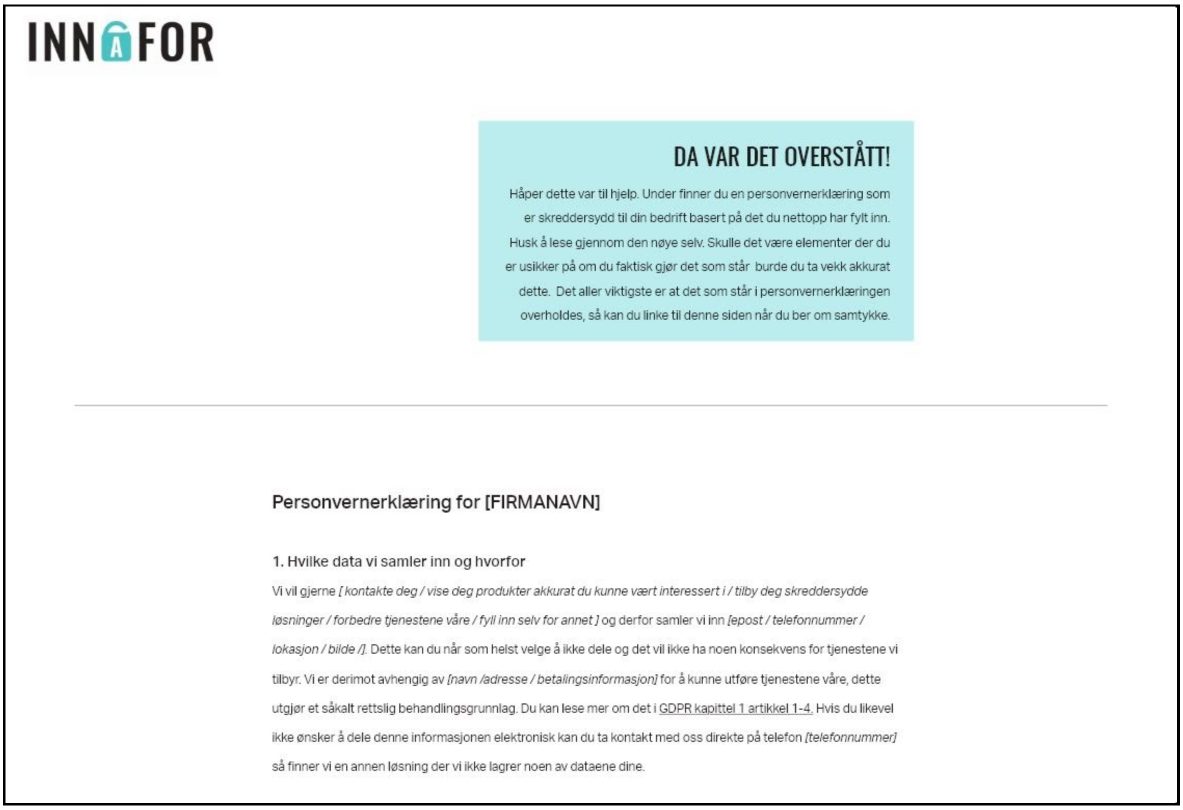
Hvis en liten bedrift samler personopplysninger om kundene sine, er de behandlingsansvarlig. Når disse dataene deles med leverandører eller eksterne tjenester som faktureringskontorer eller frilansressurser kalles dette tredjepartsleverandører, og disse blir databehandlere av personopplysningene.

□ BARE DITT FIRMA
□ TREDJEPARTSFIRMA
□ TREDJEPARTSFIRMA I UTLANDET
□ VET IKKE

Fig. 13: Final version of Innafor checkbox page.

6.3 THE FINAL RESULT PAGE

The final result page on the first design was the one that received the most critique. Not only was the text placed in tiny boxes that made it unreadable and difficult to copy (Fig 10), but there were three of these boxes and one was not mentioned at all by the testors; the box with HTML code for a popup box was scrapped. Two test users suggested the final text be one long block of paragraph text, this is a conventional way of presenting text on a website and thus it was implemented in the final design. The width of the site was also changed to a standard grid width for web (uxdesign.cc, 2019) instead of a narrow one. On top of the final page is a card with a message that finishes the conversation with the user by explaining how to use the privacy policy that was generated by their input. This ends the guided user journey through the tool (UX-writing).



DA VAR DET OVERSTÅTT!

Håper dette var til hjelp. Under finner du en personvernerklæring som er skreddersydd til din bedrift basert på det du nettopp har fylt inn. Husk å lese gjennom den nøye selv. Skulle det være elementer der du er usikker på om du faktisk gjør det som står burde du ta vekk akkurat dette. Det aller viktigste er at det som står i personvernerklæringen overholdes, så kan du linke til denne siden når du ber om samtykke.

Personvernerklæring for [FIRMANAVN]

1. Hvilke data vi samler inn og hvorfor

Vi vil gjerne *[kontakte deg / vise deg produkter akkurat du kunne vært interessert i / tilby deg skreddersydde løsninger / forbedre tjenestene våre / fyll inn selv for annet]* og derfor samler vi inn *[epost / telefonnummer / lokasjon / bilde /]*. Dette kan du når som helst velge å ikke dele og det vil ikke ha noen konsekvens for tjenestene vi tilbyr. Vi er derimot avhengig av *[navn /adresse / betalingsinformasjon]* for å kunne utføre tjenestene våre, dette utgjør et såkalt rettslig behandlingsgrunnlag. Du kan lese mer om det i GDPR kapittel 1 artikkel 1-4. Hvis du likevel ikke ønsker å dele denne informasjonen elektronisk kan du ta kontakt med oss direkte på telefon *[telefonnummer]* så finner vi en annen løsning der vi ikke lagrer noen av dataene dine.

Fig. 14: Final version of Innafor results page.

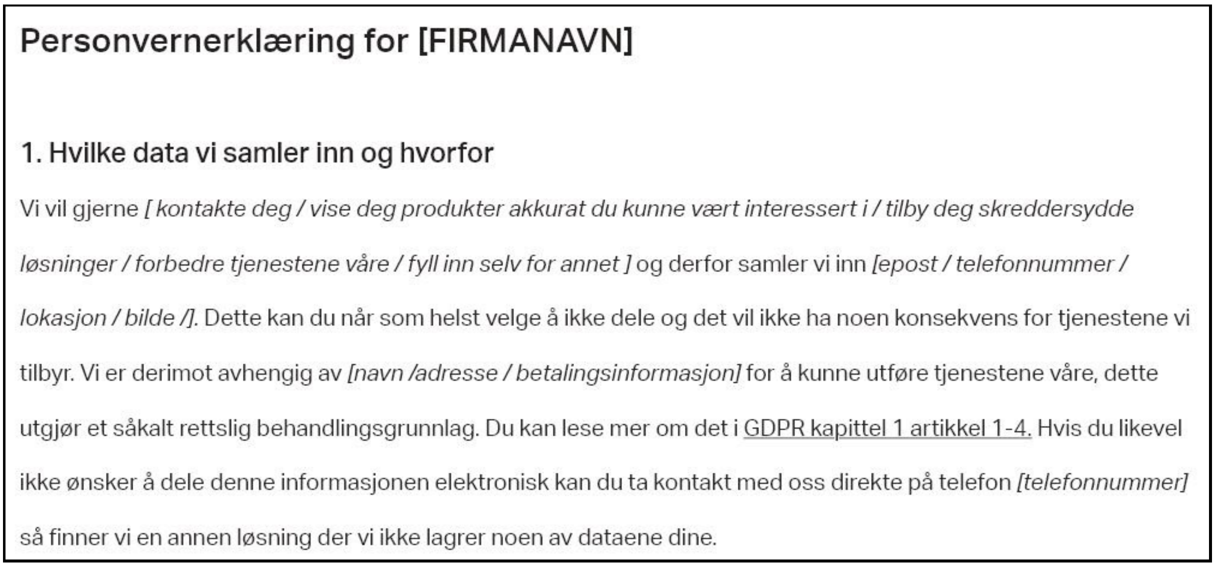
The typography of this tool was the absolute biggest problem in the first test phase. The placement, font type, size and form was all wrong according to almost every user. When deciding to place helpful tool tips next to the checkboxes, it was fairly easy to place the rest of the elements in a logical, in-line manner with a reasonable amount if white space in between. The large INNAFOR-logo at the top of the page was also shrinked in size and placed in the top left corner to create more space on the page and letting the information be the focus of attention instead of a giant logo. This was a design decision made in the heat of the moment, it was nothing the test users themselves commented on beyond saying the font was horrible. Having the logo in the top left corner os also a conventional placement of a home-button on many websites, and so it works like that in this tool as well; clicking the logo will send a user back to the first page of the site.

The font for the logo, Oswald Regular, had a low readability and so the body and checkbox text was replaced with Aktive Grotesk, an Adobe-alternative for Helvetica (creativebloq.com, 2014) which is the one of the most common sans-serif fonts in use today (Wikipedia: Helvetica, 2020). The logo has a modern look, and so the page text was kept in a sans serif as well, keeping the modern look.

6.4 THE LOGIC BEHIND THE TOOL

When doing a search through ico.org.uk for more background definitions about what this tool should include, a site with a both a quiz and an assessment checklist for small businesses showed up (ico.org.uk, 2020) This is in essence the same as what Innafor was supposed to be, a free and easy checklist for small businesses to use when they are wondering whether they are compliant and what to look out for. Considering this checklist at ICO was found during the later phase of this project, the similarities to this assessment checklist and Innafor are coincidental, and there are several differences.. Although the design of this tool looks simple, and 40% of the test users even commented on this by stating it seems like simple freeware, the complexity behind how it works is the result of carefully mapping out needs and hand picking relevant sections from the GDPR (Appendix 5). By narrowing the scope to only include small businesses, large parts of the GDPR could be excluded from the contextual data pool, making it possible to create a reliable logic behind the tool. There is only a limited number of ways a small business could handle data before having to hand it over to a compliance officer, and there is a fairly limited due diligence needed to be compliant with the GDPR when the scope is this small. Although a bare minimum of compliance seems manageable, the requirements and correct methods needed to be "innafor" (operating within the law) are still very real, and it is crucial for the small businesses to get it right. The tool developed in this project was meant to do the "dirty" work for the small business, handing them a bare minimum of what they would need to comply by barely lifting a finger. The boring part of the job has been done by sifting through the GDPR, interpreting what is relevant for a small business and then writing a privacy policy (Appendix 9) that would be general enough to cover all these areas, tailorable to any small business (Appendix 8: 10.8.6) with only minor changes to a standard text depending on what each particular business practice (limited scope gives limited possibilities, as mentioned).

The privacy policy (Appendix 9) was written from scratch based on the five questions asked on the site. First there is a paragraph about which data is being gathered and why. Here the text flow allows for the different answers given in Innafor to change the text with a few simple if/else lines of code to change key variables (words) in the text so it corresponds with the checked boxes in the form (w3schools.com, 2020).



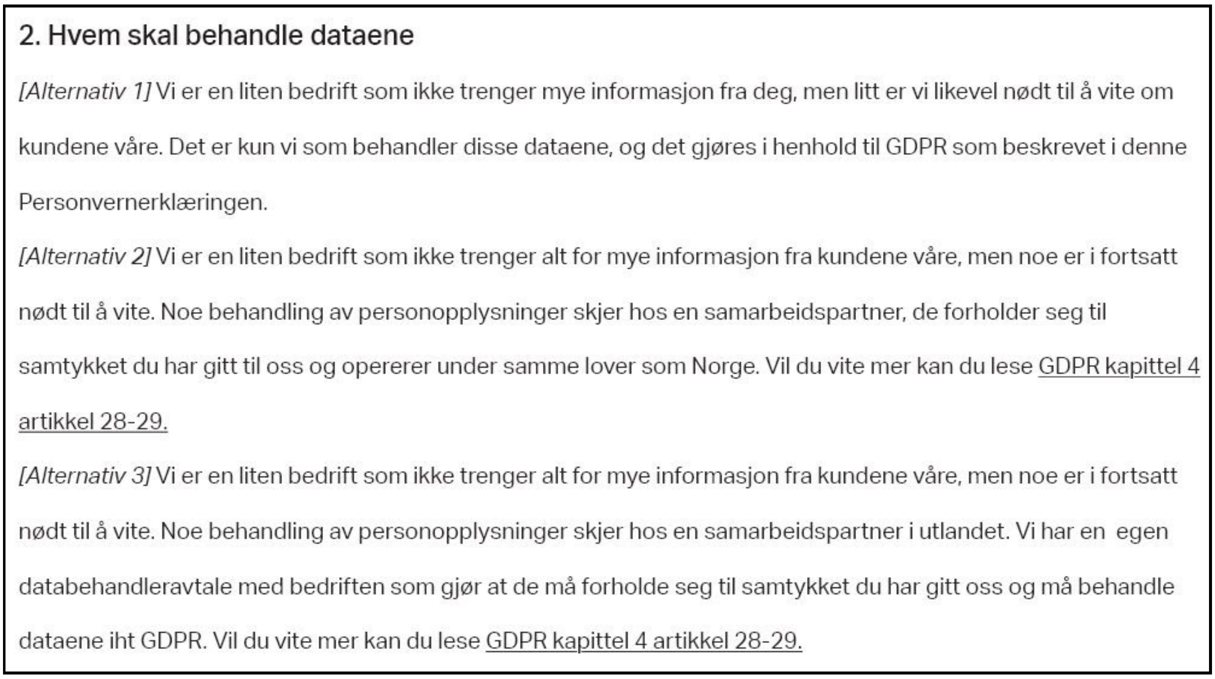
Personvernerklæring for [FIRMANAVN]

1. Hvilke data vi samler inn og hvorfor

Vi vil gjerne *[kontakte deg / vise deg produkter akkurat du kunne vært interessert i / tilby deg skreddersydde løsninger / forbedre tjenestene våre / fyll inn selv for annet]* og derfor samler vi inn *[epost / telefonnummer / lokasjon / bilde /]*. Dette kan du når som helst velge å ikke dele og det vil ikke ha noen konsekvens for tjenestene vi tilbyr. Vi er derimot avhengig av *[navn /adresse / betalingsinformasjon]* for å kunne utføre tjenestene våre, dette utgjør et såkalt rettslig behandlingsgrunnlag. Du kan lese mer om det i GDPR kapittel 1 artikkel 1-4. Hvis du likevel ikke ønsker å dele denne informasjonen elektronisk kan du ta kontakt med oss direkte på telefon *[telefonnummer]* så finner vi en annen løsning der vi ikke lagrer noen av dataene dine.

Fig 15: Text in brackets change depending on which boxes users check.

Paragraphs 2, 3 and 4 (Appendix 9) have three different entire text choices depending on which boxes have been checked. The same logic applies here; which paragraph is shown depends on code stating that *if* a certain box is checked, *then* a certain paragraph should be included in the final policy, *if else* it should not. This logic also applies to paragraph three in the policy regarding how long the data should be stored, as well as paragraph four stating how they are stored. All these paragraphs include replaceable sections.



2. Hvem skal behandle dataene

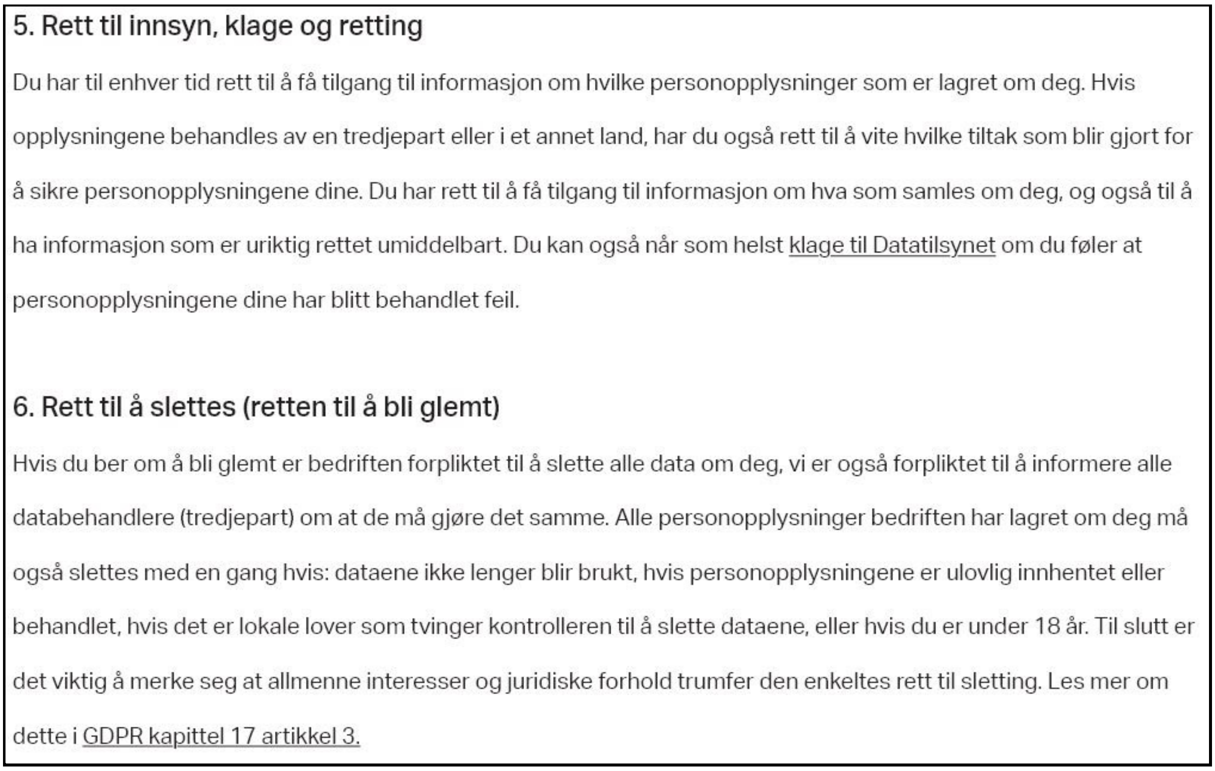
[Alternativ 1] Vi er en liten bedrift som ikke trenger mye informasjon fra deg, men litt er vi likevel nødt til å vite om kundene våre. Det er kun vi som behandler disse dataene, og det gjøres i henhold til GDPR som beskrevet i denne Personvernerklæringen.

[Alternativ 2] Vi er en liten bedrift som ikke trenger alt for mye informasjon fra kundene våre, men noe er i fortsatt nødt til å vite. Noe behandling av personopplysninger skjer hos en samarbeidspartner, de forholder seg til samtykket du har gitt til oss og opererer under samme lover som Norge. Vil du vite mer kan du lese GDPR kapittel 4 artikkel 28-29.

[Alternativ 3] Vi er en liten bedrift som ikke trenger alt for mye informasjon fra kundene våre, men noe er i fortsatt nødt til å vite. Noe behandling av personopplysninger skjer hos en samarbeidspartner i utlandet. Vi har en egen databehandleravtale med bedriften som gjør at de må forholde seg til samtykket du har gitt oss og må behandle dataene iht GDPR. Vil du vite mer kan du lese GDPR kapittel 4 artikkel 28-29.

Fig 16: Text in brackets indicate what is shown depending on boxes checked.

Paragraphs five and six are generic and refers to the general rights of all people whose data is being gathered, stored and processed: The right to access the data, have it be corrected if anything is incorrect, the right to complain to the authorities (Datatilsynet) and of course the right to be forgotten - at any time as quickly as humanly possible. There is a link to Datatilsynet sending users to an external site explaining how to complain, and another link to the gdpr.info.eu explaining the relevant article about the right to be forgotten.



5. Rett til innsyn, klage og retting

Du har til enhver tid rett til å få tilgang til informasjon om hvilke personopplysninger som er lagret om deg. Hvis opplysningene behandles av en tredjepart eller i et annet land, har du også rett til å vite hvilke tiltak som blir gjort for å sikre personopplysningene dine. Du har rett til å få tilgang til informasjon om hva som samles om deg, og også til å ha informasjon som er uriktig rettet umiddelbart. Du kan også når som helst klage til Datatilsynet om du føler at personopplysningene dine har blitt behandlet feil.

6. Rett til å slettes (retten til å bli glemt)

Hvis du ber om å bli glemt er bedriften forpliktet til å slette alle data om deg, vi er også forpliktet til å informere alle databehandlere (tredjepart) om at de må gjøre det samme. Alle personopplysninger bedriften har lagret om deg må også slettes med en gang hvis: dataene ikke lenger blir brukt, hvis personopplysningene er ulovlig innhentet eller behandlet, hvis det er lokale lover som tvinger kontrolleren til å slette dataene, eller hvis du er under 18 år. Til slutt er det viktig å merke seg at allmenne interesser og juridiske forhold trumfer den enkeltes rett til sletting. Les mer om dette i GDPR kapittel 17 artikkel 3.

Fig 17: *General sections about transparency and the right to be forgotten.*

The last paragraph (7) is one that gives data subjects the possibility to contact the small business via email or phone number, here the very first page of Innafor comes into play. The business was asked to fill in their company name, for the heading of the policy, as well as email and phone number in order for this final part of the policy to include their specific information, which is required. This information would then be entered as strings (w3schools.com, 2020) of text in the code. Once the privacy policy is copied out the small business can paste it anywhere they like, when they close the browser no data is stored online. Everything they just entered is deleted, there are no cookies on this site.

7 TESTING AND RESPONSES

7.1 TEST PHASE 2 - THE FINAL DESIGN TEST RESULTS

Interesting finds

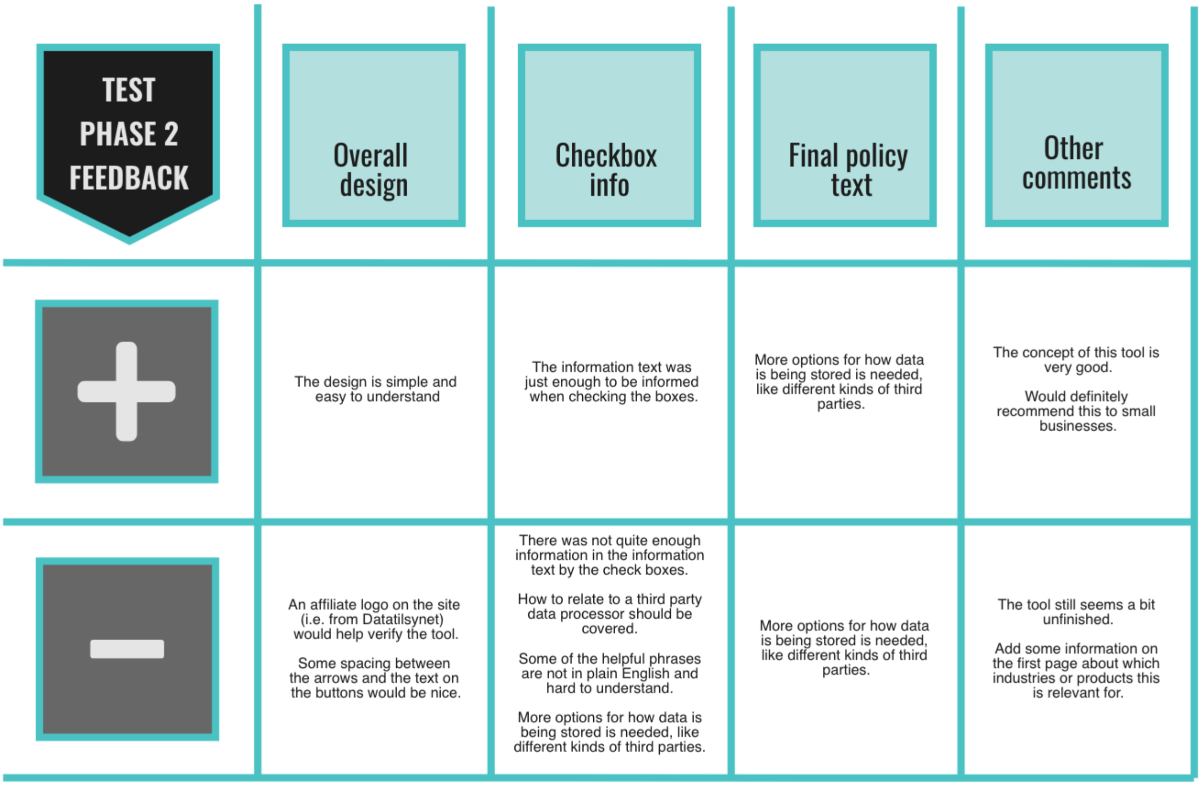
The second test revealed that most of the iteration done to the visual design was a success according to the users, which is nice, but not surprising as the first design was never meant to be polished. The interesting finds were surrounding whether the users thought the information presented in the tool was relevant, sufficient, and seemed reliable. The tailored privacy policy on the last page was deemed usable by all the test users (5) but only one user that understood the contents would also use it as-is. Another user said they would use it, although they did not understand the contents, and the last three users would use it, but change a few things first. In a further iteration asking the users what exactly they would change could uncover potential new categories of replaceable text (Fig 19) that were not included here, or it could reveal that no matter how specific a text is designed, the user or customer always wants to put their own twist on things. Further testing would have to be done to find out which is the case.

The information texts next to the checkboxes were meant to help check the right boxes by giving some context and background information from the GDPR about what they mean. They were criticized for being too simple, although some users found them to serve the intended purpose. A larger sample size of test users would reveal which point of view is representative for small businesses.

Responses to the second feedback survey

As the response survey is mostly qualitative, the answers vary in length and relevance. The most relevant feedback from the test have been sorted in Fig 18 and are listed below:

- Some of the helpful phrases are not in plain english and hard to understand.
- Add some information on the first page about which industries or products this is relevant for.
- More options for how data is being stored is needed, like different kinds of third parties.
- The design is simple and easy to understand.
- There was not quite enough information in the information text by the check boxes.
- How to relate to a third party data processor should be covered.
- An affiliate logo on the site (i.e. from Datatilsynet) would help verify the tool.
- Some spacing between the arrows and the text on the buttons would be nice.
- The information text was just enough to be informed when checking the boxes.
- The concept of this tool is very good.
- The tool still seems a bit unfinished.
- Would definitely recommend this to small businesses.



TEST PHASE 2 FEEDBACK	Overall design	Checkbox info	Final policy text	Other comments
+	The design is simple and easy to understand	The information text was just enough to be informed when checking the boxes.	More options for how data is being stored is needed, like different kinds of third parties.	The concept of this tool is very good. Would definitely recommend this to small businesses.
−	An affiliate logo on the site (i.e. from Datatilsynet) would help verify the tool. Some spacing between the arrows and the text on the buttons would be nice.	There was not quite enough information in the information text by the check boxes. How to relate to a third party data processor should be covered. Some of the helpful phrases are not in plain English and hard to understand. More options for how data is being stored is needed, like different kinds of third parties.	More options for how data is being stored is needed, like different kinds of third parties.	The tool still seems a bit unfinished. Add some information on the first page about which industries or products this is relevant for.

Fig 18: *Feedback from users in test phase 2 sorted by positive and negative*

Overall this was good feedback with no major showstoppers regarding usage or information. With another round of iteration and a final testing, this tool could be built as a free online tool for the private market. Gaining traction and trust with the intended user group would be the next hurdle to get over.

7.2 RESULTS - DID THE TOOL WORK AS INTENDED?

There are news articles, blog posts, legal experts that can help for a fee and of course the GDPR itself available online to help small businesses with GDPR-compliance, and these tools can all serve as helpful tools, but none of them are both free of charge, easy to use, and reliable at the same time. That was what Innafor was supposed to be; free, easy and reliable enough for the business to use its contents as a source of trusted information When tested two out of three goals were reached, of course the tool is free of charge, and after the last iteration it was deemed easy to use as well. When asked if they would use the privacy policy generated by the tool, there was a 50-50 response to whether it was good as-is, or needed to be edited before use. The critique seemed to be surrounding the trustworthiness of the information on the site. It was viewed as too simple, and this gave users the impression that it could be inaccurate. In reality, the information behind this tool was hand picked by relevance from the GDPR itself, carefully sifted through and then cut down to cover only the very basic minimum of information needed in order to keep the tool simple. This backfired, as the users ability to understand medium sizes blocks of fairly complex text surpasses their need for things to be “dumbed down”. It was a case of underestimating the target user.

Luckily, the information needed to make this tool even more informative and thorough is available as shown in chapter 3.1. Of this thesis, including it into this tool would only be a matter of rewriting the copy for the tool giving it more “meat on the bone” and bringing the UX-writing (careerfoundry.com, 2020) up to par. Doing this would most likely make the tool more reliable in use, but another question would be how one would make small businesses understand that they do indeed need such a tool as this. This was a part of the original thought behind the tool - having small businesses, whether they thought it to be necessary or not, take this “test” to find out if they are “Innafor” (within the law). Any small business who knows they do not handle any personal data for any user would have no reason to use this tool, and so the ones who do would in all likelihood handle data in some way and hence would need a privacy policy as well as helpful tips. Reaching small business that are in doubt like this was not something that was tested in this project, simply because it would require contacting this user group on a large scale, and getting the contact information to several small businesses from i.e. a law firm of other agencies that handle their data would ironically be in violation of the GDPR. This too, if developed, will have to be made available to the public and shared in relevant places, and then one would have to wait and see if small businesses would use it at all.

8 DISCUSSION

8.1 WHAT DID AND DID NOT WORK IN THE DESIGN

Simplicity and collaboratory design

Having the subject matter of GDPR presented in a simple and logical way was well received as a concept. Understanding the tool and how it worked was deemed a success by the testers, as they all understood how to use the tool and the goal of it. The simplicity of the design worked well, but other stylistic choices such as the font and placement of elements on the first version of the site were criticized heavily by the testers, and rightfully so. This was the purpose of having an ugly first design; the users were supposed to react to it and were asked to contribute with suggestions to how it might be better. The basic elements were there, but their placement and style were left up to the users in the second iteration. As a form of live testing this worked really well when pressed for time as the feedback was plentiful and specific.

Oversimplifying the content

The three main criteria for this project were simplicity, availability and reliability. Although a business is small, it does not mean the person in charge is unable to comprehend a subject matter of a certain complexity. It is a matter of explaining well, and so this tool could have included more details about how the GDPR is relevant on certain areas of business, and perhaps even more suggestions on how to comply in different scenarios. The oversimplification was unnecessary, and it even had a negative effect on the testers, as some lost trust in the tool because it seemed too simple. Had there been more time to map out the needs, strengths and biases of the small business user group initially, their ability and willingness to understand complex laws when explained properly might have become a consideration in the design for this project.

Responsive design

For the simplicity of the prototype there was a choice not to make the design responsive, but as a rule in UX-design one should *always* have the design responsive (w3schools.com, 2020) Several people opened the test in a mobile browser and had to start over once they realized they could not see what was on the screen at all. This led to irritation for the testers, and so the design should have been made responsive even as a prototype. Another reason for not doing this was the assumption that any small business wondering about GDPR would be sitting at their desk at work Googling the problem, however this assumption was never rooted in any survey or interview and should never have been allowed to be the basis of an important design choice such as whether to make a site responsive.

8.2 WHAT CAN BE LEARNED FROM THIS PROJECT

Recruitment

In order to do testing more effectively there should have been established a test panel made up of real small businesses, instead of recruiting repeatedly only from friends and acquaintances who happen to be in the target demographic. Finding small businesses to recruit proved difficult, but with a bit more effort into where and how they could be recruited, it might have been possible. GDPR prohibits any organisation from sharing the contact information of a small business with a student doing a school project unless specific consent has been given for this, and there is no reason why this type of consent would be a part of a standard policy. Also, when searching for larger groups of small businesses in need of GDPR help, the gatekeepers proved to be lawyers, who would be deemed competitors for the tool being developed in this project. Having them share their client base would have been illegal without them taking severe steps to facilitate the communication in a legal way, and their incentive to do so was on the negative side of zero. That being said, with some time, there might have been such a gatekeeper that would have been willing to help because of a genuine interest in developing an entry level, easy, free GDPR tool in a market that is in dire need of one. Arguably, a good lawyer would recognise that this would not compete their service, but rather complement it.

Scope and focus

When unsure about the scope of a project, the experience from this project was that one should not narrow the scope too early. Having an open mind and researching several angles of approach until the project takes on a form would be more effective than choosing a scope and focus area, only to realize it was a dead end and then having to start all over with a different approach. This was extremely time consuming and although some of the insights from the first part of this project proved useful, a lot of the work done initially was a proper waste of time.

Dare to ask

The big league resources on this topic are available and willing to help, this became evident once the project was done and caught the attention of one of them. Daring to reach out to Eva Jarbekk or Torgeir Waterhous early on would most likely have been very fruitful, instead of trying to figure out a noble way of gathering data and insights alone. Pride mixed with intimidation stood in the way. When doing projects like this, any student should not be afraid to reach out, given the topic and idea is specific and can be approached by a professional in a constructive way. A teacher from NTNU could help narrow a scope or find the words in an email, but sending that email and gathering all the knowledge and insights and help available is an absolute advantage and not something a student should be afraid of.

8.3 FURTHER DEVELOPMENT

When testing the prototype, one of the testers who participated in both the first and the second phase emailed and explained that his company has been developing a backend solution that would be extremely compatible with the concept developed in this project.

"We have a slightly larger system for the SMB market in mind. You have the front of the system where the documents can be generated. We have thought of a complete tool for GDPR compliance which will ensure that GDPR is taken care of completely in the company. This relates to all handling / exchange of personal data, and even role management for the controller or data processor during data processing. (...) With your product we saw a match with our GDPR concept. We are, after all, a bunch of old farts and should not front these ideas. We will help with everything else, development, financing, contact networks etc."

Going forward, a start-up will be established and the company will go on to create a project gathering funds and interest for this tool. The plan for the summer following the delivery of this thesis looks like this:

1. Establish the company (Startup).
2. Establish a formal agreement on the intention and plan of the company including onboarding of partners (shareholder register).
3. Application Innovation Norway for Market Clarification.
4. Validate the market (Input for writing the pre-project application) .
5. Pre-project (Implementation including enrichment of MVP).
6. Validation / Experimentation against main project application.

If all goes to plan, a MVP (Wikipedia: minimum viable product, 2020) will be developed during the summer of 2020 and then developed further in the fall.

9 REFERENCES

Bedrebedrift.no (2018) *GDPR for små bedrifter: Steg 1 (protokoll).* Available at https://www.bedrebedrift.no/blog/gdpr-for-sma-bedrifter-steg-1
(Accessed February 2020)

Bedrebedrift.no (2018) *GDPR for små bedrifter: Steg 3 (databehandleravtale).* Available at https://www.bedrebedrift.no/blog/gdpr-for-sma-bedrifter-steg-3
(Accessed March 2020)

Bedrebedrift.no (2020) *GDPR SOS.* Available at https://www.bedrebedrift.no/gdpr-sos#section-1575706443527 (Accessed February 2020)

Careerfoundry.com (2020) *What does a UX writer actually do?* Available at https://careerfoundry.com/en/blog/ux-design/ux-writing-what-does-a-ux-writer-actually-do/ (Accessed May 2020)

Cnil.fr (2919) *The CNIL´s restricted committee imposes a financial penalty of 50 Million Euros against GOOGLE LLS.* Available at https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (Accessed May 2020)

Creativebloq.com (2014) *20 top web fonts.* Available at: https://www.creativebloq.com/typography/20-top-web-fonts-31410869 (Accessed May 2020)

Datatilsynet.no (2019) *Vurdering av personvernkonsekvenser.* Available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/
(Accessed April 2020)

Datatilsynet.no (2018) *Når og hvordan skal jeg melde avvik.* Available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/nar-skal-jeg-melde-avvik/
(Accessed April 2018)

Datainspektionen.se (2020) *Tilsyn enligt EU´s dataskyddförordning 2016/679 – Googles antering av begäranden om borttagande från dess söktjänster.* Available at https://www.datainspektionen.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf (Viewed April 2020)

Datatilsynet.no (2018) *Protokoll over behandlingsaktiviteter.* Available at (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/) (Accessed march 2020)

Datatilsynet.no (2018) *Innebygget personvern.* Available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/ (Accessed February 2010)

Datatilsynet.no (2018) *Etablere internkontroll. Available* at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/
(Accessed March 2020)

Datatilsynet.no (2019) *Fastsette formål.* Available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/fastsette-formal/
(Accessed March 2020)

Datatilsynet.no (2019) *Behandlingsgrunnlag.* Available at (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/)
(Accessed March 2020)

Datatilsynet.no (2018) *Leggje til rette for brukarens rettar.* Available at (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/legge-til-rette-for-rettigheter/)
(Accessed March 2020)

Datatilsynet.no (2018) *Personvernombud.* Available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/ (Accessed March 2020)

Datatilsynet.no (2018) *Databehandleravtale.* Available at (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/) (Accessed March 2020)

Datatilsynet.no (2018) *Spesielt om overføring av data til utlandet.* Available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/
(Accessed March 2020)

E24.no (2018) *Små bedrifter sliter med GDPR: -Overveldende komplisert regelverk.* Available at https://e24.no/teknologi/i/G1EzaV/smaa-bedrifter-sliter-med-gdpr-overveldende-komplisert-regelverk(Accessed February 2020)

Fhi.no (2020) *Avstand, karantene og isolering.* Available at (https://www.fhi.no/nettpub/coronavirus/fakta/avstand-karantene-og-isolering/ (Accessed May 2020)

Forbes.com (2018) *Flourishing among the fjords – Norway´s dynamic startup scene.* Available at https://www.forbes.com/sites/alisoncoleman/2018/10/05/flourishing-among-the-fjords-norways-dynamic-startup-scene/#3788b3c95efb
(Accessed April 2020)

Gdprdokumentasjon.no (2018) *Om GDPR.* Available at https://www.gdprdokumentasjon.no/om-gdpr
(Accessed March 2020)

GDPR.EU (2019) *2019 GDPR.EU Small business Survey.* Available at https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf (Downloaded April 2020)

GDPR-info.eu (2018) *GDPR.* Available at http://gdpr-info.eu (Accessed February 2020)

Gilbert, K. (2016) *The Co-Design Workshop: The Facilitator's Pocket Guide.* Available at https://connection.domain7.com/the-co-design-workshop-the-pocket-facilitators-guide-e36a6c9e08d4
(Accessed March 2020)

Gray, D., Brown, S., Macanufo, J. (2010) *Game Storming - a playbook for innovators, rulebreakers and changemakers* (1st edt) O'Reilly Media Inc., CA USA.

Ico.org.uk (2020) *How well do you comply with data protection law: an assessment for small business owners and sole traders.* Available at https://ico.org.uk/for-organisations/business/assessment-for-small-business-owners-and-sole-traders/
(Accessed May 2020)

Jarbekk, E., Sommerfeld, S., (2019) Personvern og GDPR i praksis (1. utg) Cappelen Damm Akademisk, Oslo

Lansborg, K. F. H. (2019) *Will Privacy by Design principles endure GDPR compliance in Smart City innovation.* Paper written for Interaction Design Specialization, NTNU Gjøvik.

NHO.NO (2020) *Fakta om små og mellomstore bedrifter.* Available at https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/ (Accessed April 2020)

Slideshare.net (2016) *Co-design Workshop.* Available at https://www.slideshare.net/userspots/codesign-workshop (Accessed February 2020)

Statisticshowto.com (2014) *Snowball sampling.* Available at: https://www.statisticshowto.com/snowball-sampling/ (Accessed February 2020)

Stickdorn, M., Hormess, M., Lawrence, A., & Schneider, J. (Eds.) (2018) *This is Service Design Doing* (1st edt) O'Reilly Media Inc., CA USA.

Uxdesign.cc (2019) *Responsive grids and how to actually use them.* Available at: https://uxdesign.cc/responsive-grids-and-how-to-actually-use-them-970de4c16e01 (Accessed May 2020)

Uxplanet.org (2017) UX Writing. *Let User Interface Speak.* https://uxplanet.org/ux-writing-let-user-interface-speak-774f80c0a94d (Accessed May 2020)

Who.int (2020) *Novel Coronavirus 2019.* Available at https://www.who.int/emergencies/diseases/novel-coronavirus-2019 (Accessed May 2020)

Wikipedia (2020) *Google Forms.* Available at https://en.wikipedia.org/wiki/Google_Forms (Accessed May 2020)

Wikipedia (2019) *General Data Protection Regulation.* Available at https://en.wikipedia.org/wiki/General_Data_Protection_Regulation (Accessed March 2020)

Wikipedia (2020) *Helvetica.* Available at https://en.wikipedia.org/wiki/Helvetica (Accessed May 2020)

Wikipedia (2020) *MVP Minimum Viable product.* Available at: https://en.wikipedia.org/wiki/Minimum_viable_product (Accessed June 2020)

W3schools.com (2020) *Java If… Else.* Available at https://www.w3schools.com/java/java_conditions.asp (Accessed May 2020)

W3schools.com (2020) *JavaScript String Reference.* Available at https://www.w3schools.com/jsref/jsref_obj_string.asp (Accessed May 2020)

W3schools.com (2020) *HTML Responsive Web Design.* Available at https://www.w3schools.com/html/html_responsive.asp (Accessed May 2020)

Zhaohao Sun & Yanxia Huo (2019) *The Spectrum of Big Data Analytics, Journal of Computer Information Systems,* DOI: 10.1080/08874417.2019.1571456

10 APPENDIX

APPENDIX 1 - SURVEY SERVICE DESIGNERS

Anonymous survey for service designers

Where do you work?

Open answer.

What is your job title?

Service Designer

UX-Designer

Frond-End developer

Security advisor

Legal advisor

IT-security

Other

What kind of projects are you working on at the moment?

Open answer

Do you ever encounter challenges with GDPR in your work?

Yes, it has halted projects completely.

Yes, but we have legal advisors look at it and they figure it out.

Yes, we usually find a workaround by reading up on the issue ourselves.

No, we simply submit our work to the compliance manager to get approval.

No, we rarely design services where sensitive data are involved.

Could you elaborate a bit about your experience with GDPR in your work?

Open answer.

Have you received any formal training concerning handling sensitive information?

Yes, my employer provided extensive training.

Yes, my employer held a meeting/crash course.

Yes, I received mandatory readings about the subject from my employer.

Yes, I was granted leave from my employer to participate in a seminar/training.

Yes, I made sure to inform myself during business hours.

Yes, I used my free time to learn about it.

No, I Google whatever I need to know.

No, my colleagues and I discuss it and learn from each other.

No, the compliance manager handles everything.

Have you heard about Privacy by Design? (innebygget personvern)

Yes

No

If you answered Yes to the last question, great! If not, the short description of Privacy by Design is basically when a product is designed with privacy as a priority, along with whatever other purposes the system serves. It is when privacy by default is incorporated into the tech and systems themselves. Knowing this, would you say this is a practice you and your coworkers have in place already?

Yes, definitely!

Yes, I'd say we do this to some degree.

It's a nice thought, but very hard to do retroactively (e.g. when redesigning existing apps).

No, it's not something we do actively, even with new projects, but I think we should.

No, and I don't think these principles work very well in real life.

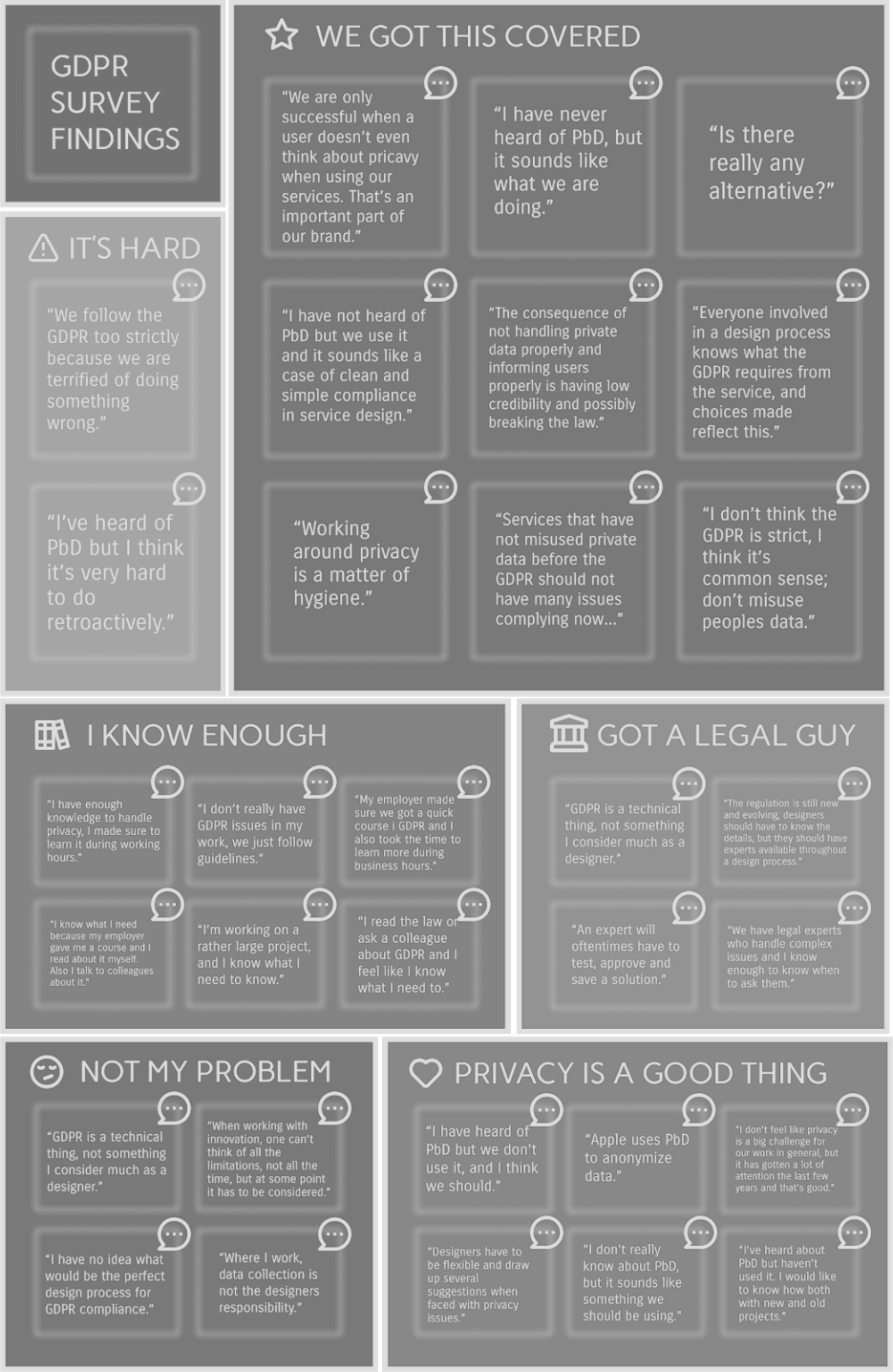
Whatever your answer was on the last question, could you please elaborate on your experience with Privacy by Design?

Open answer.

How do you envision a perfect design process, in regards to handling sensitive data?

Open answer.

APPENDIX 2 – SERVICE DESIGN SURVEY FINDINGS



GDPR SURVEY FINDINGS

IT'S HARD

"We follow the GDPR too strictly because we are terrified of doing something wrong."

"I've heard of PbD but I think it's very hard to do retroactively."

WE GOT THIS COVERED

"We are only successful when a user doesn't even think about pricavy when using our services. That's an important part of our brand."

"I have never heard of PbD, but it sounds like what we are doing."

"Is there really any alternative?"

"I have not heard of PbD but we use it and it sounds like a case of clean and simple compliance in service design."

"The consequence of not handling private data properly and informing users properly is having low credibility and possibly breaking the law."

"Everyone involved in a design process knows what the GDPR requires from the service, and choices made reflect this."

"Working around privacy is a matter of hygiene."

"Services that have not misused private data before the GDPR should not have many issues complying now..."

"I don't think the GDPR is strict, I think it's common sense; don't misuse peoples data."

I KNOW ENOUGH

"I have enough knowledge to handle privacy, I made sure to learn it during working hours."

"I don't really have GDPR issues in my work, we just follow guidelines."

"My employer made sure we got a quick course i GDPR and I also took the time to learn more during business hours."

"I know what I need because my employer gave me a course and I read about it myself. Also I talk to colleagues about it."

"I'm working on a rather large project, and I know what I need to know."

"I read the law or ask a colleague about GDPR and I feel like I know what I need to."

GOT A LEGAL GUY

"GDPR is a technical thing, not something I consider much as a designer."

"The regulation is still new and evolving, designers should have to know the details, but they should have experts available throughout a design process."

"An expert will oftentimes have to test, approve and save a solution."

"We have legal experts who handle complex issues and I know enough to know when to ask them."

NOT MY PROBLEM

"GDPR is a technical thing, not something I consider much as a designer."

"When working with innovation, one can't think of all the limitations, not all the time, but at some point it has to be considered."

"I have no idea what would be the perfect design process for GDPR compliance."

"Where I work, data collection is not the designers responsibility."

PRIVACY IS A GOOD THING

"I have heard of PbD but we don't use it, and I think we should."

"Apple uses PbD to anonymize data."

"I don't feel like privacy is a big challenge for our work in general, but it has gotten a lot of attention the last few years and that's good."

"Designers have to be flexible and draw up several suggestions when faced with privacy issues."

"I don't really know about PbD, but it sounds like something we should be using."

"I've heard about PbD but haven't used it. I would like to know how both with new and old projects."

APPENDIX 3 - INFORMED CONSENT FORM

Vil du delta i forskningsprosjektet

«Bruk av innebygget personvern for å designe GDPR-robuste tjenester»?

NTNU

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kartlegge smertepunkter rundt å designe digitalt under det nye personvernreglementet i GDPR. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Dette er et masterprosjekt i interaksjonsdesign ved NTNU på Gjøvik. Prosjektet handler om hvordan gjøre GDPR etterfølgelse enklere for utviklere og digitale designere. Formålet med dette prosjektet er å kartlegge smertepunkter i å designe rundt personvern, og å utforme et verktøy som kan gjøre det lettere å implementere innebygget personvern i designprosessen. Dataene i prosjektet skal brukes til å kartlegge dagens praksis, skape et helhetsbilde av utfordringer og smertepunkter, og få et solid utgangspunkt for å utvikle et godt hjelpemiddel.

Hvem er ansvarlig for forskningsprosjektet?

Karen Felicia Hjertstedt Lansborg er hovedansvarlig for prosjektet. Frode Volden ved NTNU Gjøviker også medansvarlig som studentveileder for prosjektet.

Hvorfor får du spørsmål om å delta?

Du er blitt kontaktet via felles kontakter ved NTNU eller fordi du jobber på en arbeidsplass som har fått spørsmål direkte til avdelingsleder om det finnes fagpersoner som er villig til å delta i denne undersøkelsen.

Hva innebærer det for deg å delta?

Som fagperson vil du bli bedt om å besvare 7 spørsmål i et åpent personlig intervju. Det vil være
lydopptak på intervjuet for å bedre få med alle detaljer, både undersøkelsen og intervjuet er anonymt og lydopptaket slettes ved prosjektets slutt i mai 2020. Du vil primært bli spurt om din erfaring med GDPR og å designe i og/eller for mindre bedrifter.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil da bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Innsamlede data vil bli benyttet kun for å avdekke hva som fungerer og ikke fungerer i dagens
designpraksis i mindre foretak. I utgangspunktet er ingen sensitive personopplysninger nødvendig å samle inn i denne fasen av prosjektet, men skulle det dukke opp identifiserende opplysninger vil disse bli anonymisert slik at ingen navn eller andre personlige detaljer blir lagret. Lydopptak vil bli brukt for analyse av funn under intervjuer. Opptaket vil ikke bli delt med andre enn prosjekteier Karen Felicia Hjertstedt Lansborg, og studentveileder for prosjektet på NTNU Gjøvik, Frode Volden, og din identitet vil ikke bli assosiert med dine data. Opptaket vil bli slettet etter prosjektets fullførelse.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Prosjektet skal etter planen avsluttes 31.05.2020 og alle lydopptak vil da bli slettet. Alle signerte
samtykkeerklæringer vil bli oppbevart skriftlig og nedlåst så lenge prosjektet pågår, og makuleres når prosjektet er ferdigstilt.

Dine rettigheter

Du vil ikke kunne identifiseres i datamaterialet, men du har fortsatt rett til å:

1. Ha innsyn i hvilke personopplysninger som er registrert om deg.
2. Få rettet personopplysninger om deg.
3. Få slettet personopplysninger om deg.
4. Få utlevert en kopi av dine personopplysninger (dataportabilitet).
5. Sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.
På oppdrag fra NTNU Gjøvik har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
NTNU Gjøvik
ved Karen Felicia Hjertstedt Lansborg (kflansbo@stud.ntnu.no)
eller Frode Volden (frodv@ntnu.no)

Personvernombud ved NTNU er Thomas Helgesen (thomas.helgesen@ntnu.no)
NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no)
eller telefon: 55 58 21 17.

Med vennlig hilsen
Prosjektansvarlig,
Karen Felicia Hjertstedt Lansborg

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «Bruk av innebygget personvern for å designe GDPR-robuste tjenester», og har fått anledning til å stille spørsmål.

Jeg samtykker til: å delta i personlig intervju.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca 31. mai 2020

(Prosjektdeltager, dato)

APPENDIX 4 - FEEDBACK SURVEY PHASE 1

Tilbakemelding på "Innafor"

Etter å ha testet "innafor" verktøyet er det fint om du kan gi en tilbakemelding. Alle tilbakemeldinger er anonyme og vil kun brukes til å forbedre verktøyet og vurdere hvorvidt det
har ønsket effekt.

1. Hva jobber du med sånn cirka? Flere svar mulig.

Webdesign
UX-design
Tjenestedesign
Prosjektledelse
Front-end
Noe annet i samme baner
Noe helt annet

**2. Har du støtt på personvernproblematikk i arbeid eller studier etter GDPR trådte i
kraft?**

Ja, ofte.
Veldig lite.
Nei, aldri.

3. Forstod du hvordan du skal bruke Innafor-verktøyet?

Ja.

Ikke med en gang, men etterhvert.

Nei.

4. Testen huket av for deg og svaret på siste side er basert på det som ble huket av.
Med det i tankene, hvor nyttig syns du informasjonen på den siste siden var?

Lite nyttig, jeg kunne det fra før.

1 2 3 4 5

Veldig nyttig, dette trenger jeg!

5. Er det annen type informasjon du skulle ønske var del av resultatet?

Åpent svar:

6. Ville du brukt dette verktøyet om det fantes?

Aldri.

1 2 3 4 5

Hele tiden!

7. Enten du selv ville brukt dette verktøyet selv eller ei, ville du anbefalt det til andre?

Definitivt!

Hvis det var litt bedre (forslag til forbedringer kan gis straks).

Nei.

8. Hvilke av disse utsagnene passer best med ditt inntrykk av Innafor-verktøyet?

Veldig enkelt, deilig å få ting servert.
For enkelt, stoler ikke helt på resultatet.
Det virker litt uferdig, men har potensiale.
Dette har jeg ventet på! Launch asap!
Ser ikke helt bruksområdet for dette.
Funksjonen er grei, men designet er forferdelig.
Bra funksjon, flott design, veldig nyttig, kjør på!

9. Var det noe du syns var spesielt vanskelig å forstå teknisk?

Åpent svar:

10. Var det noe ved det visuelle designet du ville endret?

Åpent svar:

11. Har du andre tilbakemeldinger?

Åpent svar:

12. Takk for hjelpen
Bare hyggelig!
Lykke til!

This content is neither created nor endorsed by Google Forms

APPENDIX 5 - RELEVANT GDPR SECTIONS

Chapter 1: “General Provisions”

Art. 3 - “Territorial scope”

This article explains that the regulation applies to any “Controller" i.e. a company that processes the personal data of a person located in the EU, whether or not the company is based in the EU. It also explains that this applies to any offered service, be it free or not, as well as monitoring people's behaviour without offering or selling anything. (https://gdpr-info.eu/art-3-gdpr/)

Art. 4 - “Definitions”

This article explains what is defined as personal data, and what is defined as the processing of this. Personal data is defined as e.g name, an identification number, location data, an online identifier, very specific physical description, or anything describing the identity of a person. Processing data is defined as collecting or recording information, organizing or structuring data, storing or adapting it. Finding old data in a file system or using it in any way, as well as sharing it or even deleting it is regarded as the processing of data. Several points in this article are not relevant for small businesses, but the explanation of what a “Controller” means is explained as a natural or legal person who determines the purpose and ways of handling data. The article also explains that a third party is any person, agency authorized by the controller to process personal data. Consent is defined as an affirmative action given freely by a user indicating specifically their wishes regarding the data collected. A personal data breach is when the data collected is lost, leaked, deleted by accident or transmitted to third parties without the users (data subjects) consent. (https://gdpr-info.eu/art-4-gdpr/)

Chapter 2: “Principles”

Art. 6 - “Lawfulness of processing”

In order for the processing of data to be legal, there needs to be a reason to do it. Content has been given, processing the data is necessary to perform a contract, the controller has a legal obligation to handle the data, handling the data is necessary to protect a data subject, it is in the public interest to process the data, and/or (most importantly) there simply is a legitimate interest to handle the data, one that does not interfere with the data subjects legal rights or safetly. Processing of data should take place only if one or many of these things apply. (https://gdpr-info.eu/art-6-gdpr/)

Chapter 3: “Rights of the data subject”

Art. 13 - “Information to be provided where personal data are collected from the data subject”

When collecting data, the “Controller” needs to inform the data subject of who they are and how they can be contacted, why the data is being collected, where the data is being processed and why, how long the data will be stored, the data subjects right to access, change delete the information stored about them, or to have the information sent to them, their right to withdraw consent at any time or file a complaint with a higher authority. If the “Controller” intends to use the data for other purposes than it was originally collected, the data subject needs to be informed of this and give specific consent for this new use. (https://gdpr-info.eu/art-13-gdpr)

Art. 15 - “Right of access by the data subject”

As mentioned, the user (data subject) has a right to access information about what personal data about them is being gathered and processed any time. Also, if the data is being sent to a third party or another country, the data subject has a right to know what measures are taken to secure their personal data. If a user asks for more than one copy of the personal data being processed about them, the “Controller” (small business) can charge a small fee for this. The data shall be given in “ a commonly used electronic form”. (https://gdpr-info.eu/art-15-gdpr/)

Art. 16 - “Right to rectification”

The data subject has the right to access information about what is being gathered about them, and also to have information that is incorrect rectified immediately. https://gdpr-info.eu/art-16-gdpr/

Art. 17 - “Right to erasure (‘right to be forgotten’)

This is one of the most important points in the GDPR. A controller (the small business) has to erase everything about the data subject (user/customer) right away if: the data is no longer being used, if the data subject asks for it, if the data subject has specific reasons for the data not to remain, if the personal data has been unlawfully obtained or processed, if there are local laws compelling the controller to erase the data, or if the data subject is under age and part of society services. If the data subject asks to be forgotten, the controller is also obliged to inform all data processors (third party) that this is the case. Finally, it is important to note that public interest and legal matters trumf the individual's right to erasure. https://gdpr-info.eu/art-17-gdpr/

Art. 18 - “Right to restriction of processing”

If a data data subject and a controller cannot come to an agreement about erasure or rectification, the data subject has a right to restrict the processing of the data in the time it takes to solve the dispute. Should there be legal reasons for the data to be used despite this, the data subject will have to give consent on a case to case basis.

Art. 19 - “Notification obligation regarding rectification or erasure of personal data or restriction of processing”

This is also one of the most important articles to note. Where there has been a rectification or erasure of personal user data, the data controller is obliged to inform all third parties (data processors) to which the personal data has been disclosed. The data subject also has the right to know who these parties are at any time. If informing all third parties requires a disproportionate amount of work however, the data controller is not obliged to do this. (https://gdpr-info.eu/art-19-gdpr/)

Art. 20 - “Right to data portability”

This article refers to the data subject’s right to have the information handled about them by a data controller (in this case a small business) sent to them in a format that is readable for a regular personal computer or a human eye. The person can then send this data to any other party if they choose. Again, all of this only applies if it does not interfere with the greater good of the public or a legal matter. (https://gdpr-info.eu/art-20-gdpr/)

Art. 21 - ”Right to object”

This is one of the articles that has perhaps been most talked about surrounding the GDPR. In this it is stated that all data subjects have the right to object to their data being used for profiling for marketing purposes, and that any data controller has to inform the subject of this in a clear and understandable way separate from any other information on the site, before proceeding to collect any data. This article is the reason websites have a popup asking for permission to collect cookies. The data subject also has the right to object to any handling of their data regardless of what it is being used for, unless it interferes with public interest or legal matters. Should personal information be necessary to carry out an operation for a certain customer service, this information should be deleted directly after being used so as to avoid being subject to further processing. (https://gdpr-info.eu/art-21-gdpr/)

Art. 22 - “Automated individual decision-making, including profiling”

Any data collected about a subject can be used for profiling which is used in automated decision making such as tailored ads or search results, the data subject has the right not to be the subject of this. Automated processes used for profiling based on a data subject's personal data can be necessary in order to carry out the terms of a contract, if that is the case, the data controller needs to implement measures to ensure the integrity of the personal data. The data subject might have given consent at a previous stage, if that is the case, the subject has the right to withdraw consent at any time and the data controller will have to inform all third party data processors of this so all processing leading to automated decisions is halted. (https://gdpr-info.eu/art-22-gdpr/)

Art. 23 - “Restrictions”

In the sections above, public interest and legal matters have been mentioned a few times as they may interfere with the individuals rights according to the GDPR. In this article, the items that make up these exceptions are listed as:

- National security.
- Defence.
- Public security
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

- Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security.
- The protection of judicial independence and judicial proceedings.
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions.
- A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority (...).
- The protection of the data subject or the rights and freedoms of others.
- The enforcement of civil law claims.

The data subject has the right to be informed in case these restrictions are relevant to the handling of their data, including the reasons for the restriction and the scope of the continued handling of their data.

(https://gdpr-info.eu/art-24-gdpr/)

Chapter 3: “Controller and processor”

Art. 28 - “Processor”

If a small business gathers personal data about their customers, then they are the controllers. When this data is shared with vendors or external services such as billing offices or freelance resources for projects, then these parties become processors of this data. In the case of third parties processing the data collected, these parties have to prove that adequate measures to ensure GDPR compliant data handling are in place. If a data processor is based in a country where the local laws include the GDPR, then this is sufficient. If however the data is collected and is being sent to a country where the local laws surrounding handling of personal information are less strict than then GDPR, a separate contract ensuring the correct handling of data will have to be signed before any data is processed here.

Art. 29 - “Processing under the authority of the controller or processor”

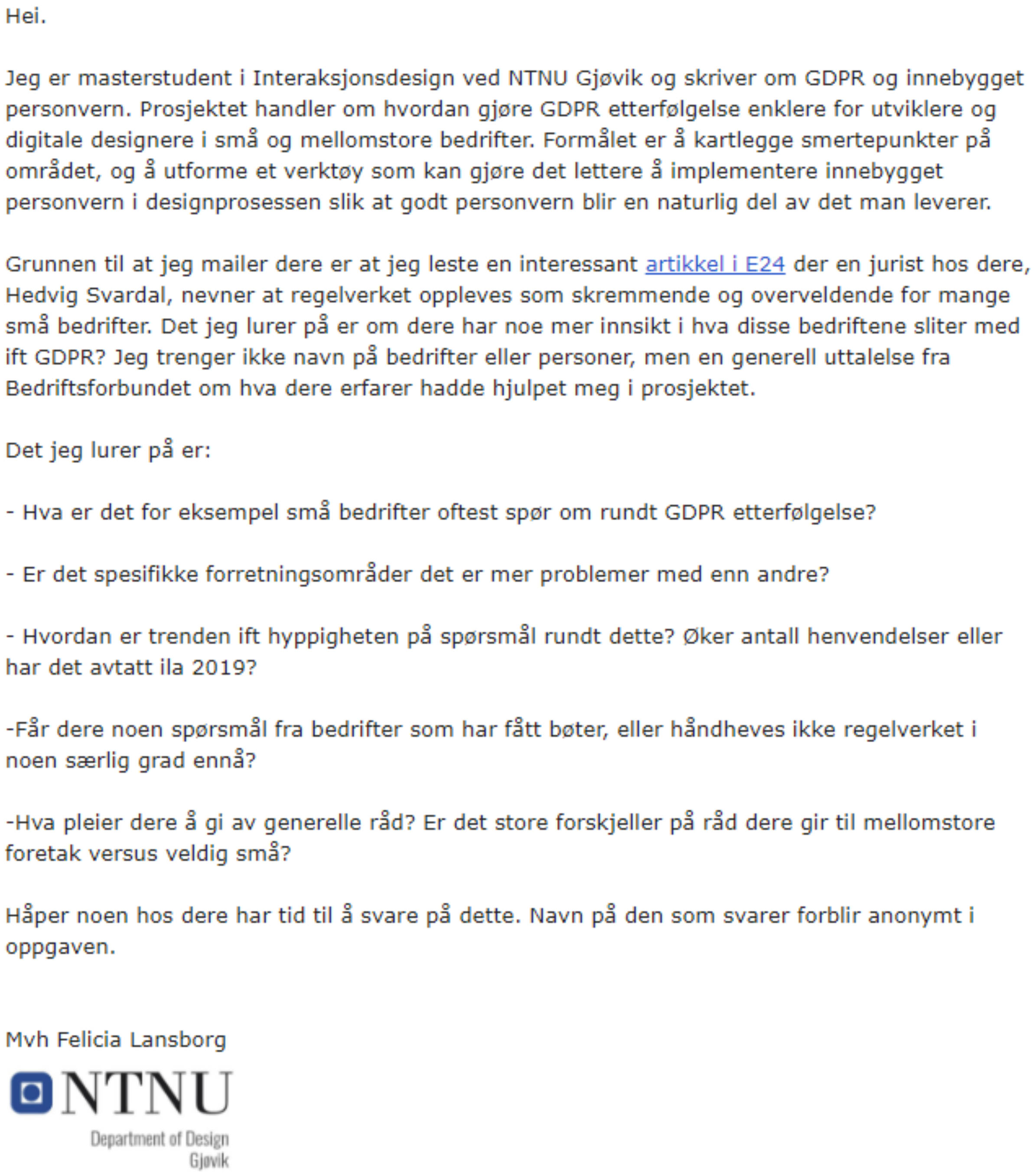
Any processing of the data will have to be authorized by the controller or the processor, which means the data shall only be used for that which it was intended and only for the amount of time it was said to be processed. Any handling of data beyond this is outside of what the data subject has consented to.

Chapter 8: “Remedies, liability and penalties”

Art. 83 - “General compensation and liability”

The final relevant point for the demographic of small businesses is the one about administrative fines. Here, it is stated that the fine imposed should be proportionate to the nature, gravity and duration of the infringement, as well as the number of people it affects. Action taken by the data processor to mitigate the damages done will also be a factor that will act in their favour. There are also several other factors that affect the fine, such as whether the data controller informed about the breach themselves or was reported by others, or whether they have been asked to improve at an earlier time and have not done so, the level of cooperation shown by the data controller, or whether there was financial gain from ignoring the proper handling of personal data. The fines can be 4% of the companies revenue upto €20 000 000.

APPENDIX 6 - SMALL BUSINESS INTERVIEW



Hei.

Jeg er masterstudent i Interaksjonsdesign ved NTNU Gjøvik og skriver om GDPR og innebygget personvern. Prosjektet handler om hvordan gjøre GDPR etterfølgelse enklere for utviklere og digitale designere i små og mellomstore bedrifter. Formålet er å kartlegge smertepunkter på området, og å utforme et verktøy som kan gjøre det lettere å implementere innebygget personvern i designprosessen slik at godt personvern blir en naturlig del av det man leverer.

Grunnen til at jeg mailer dere er at jeg leste en interessant artikkel i E24 der en jurist hos dere, Hedvig Svardal, nevner at regelverket oppleves som skremmende og overveldende for mange små bedrifter. Det jeg lurer på er om dere har noe mer innsikt i hva disse bedriftene sliter med ift GDPR? Jeg trenger ikke navn på bedrifter eller personer, men en generell uttalelse fra Bedriftsforbundet om hva dere erfarer hadde hjulpet meg i prosjektet.

Det jeg lurer på er:

- Hva er det for eksempel små bedrifter oftest spør om rundt GDPR etterfølgelse?

- Er det spesifikke forretningsområder det er mer problemer med enn andre?

- Hvordan er trenden ift hyppigheten på spørsmål rundt dette? Øker antall henvendelser eller har det avtatt ila 2019?

-Får dere noen spørsmål fra bedrifter som har fått bøter, eller håndheves ikke regelverket i noen særlig grad ennå?

-Hva pleier dere å gi av generelle råd? Er det store forskjeller på råd dere gir til mellomstore foretak versus veldig små?

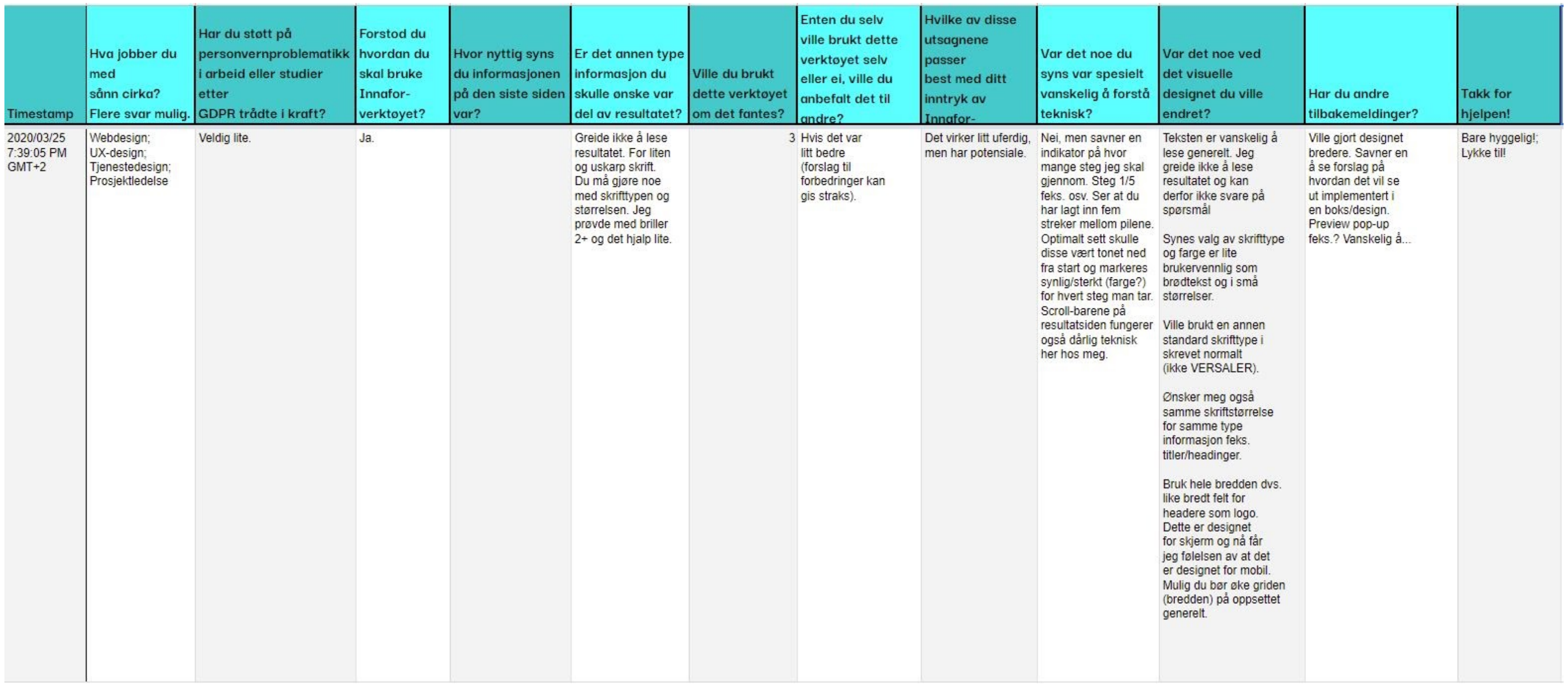
Håper noen hos dere har tid til å svare på dette. Navn på den som svarer forblir anonymt i oppgaven.

Mvh Felicia Lansborg

NTNU
Department of Design
Gjøvik

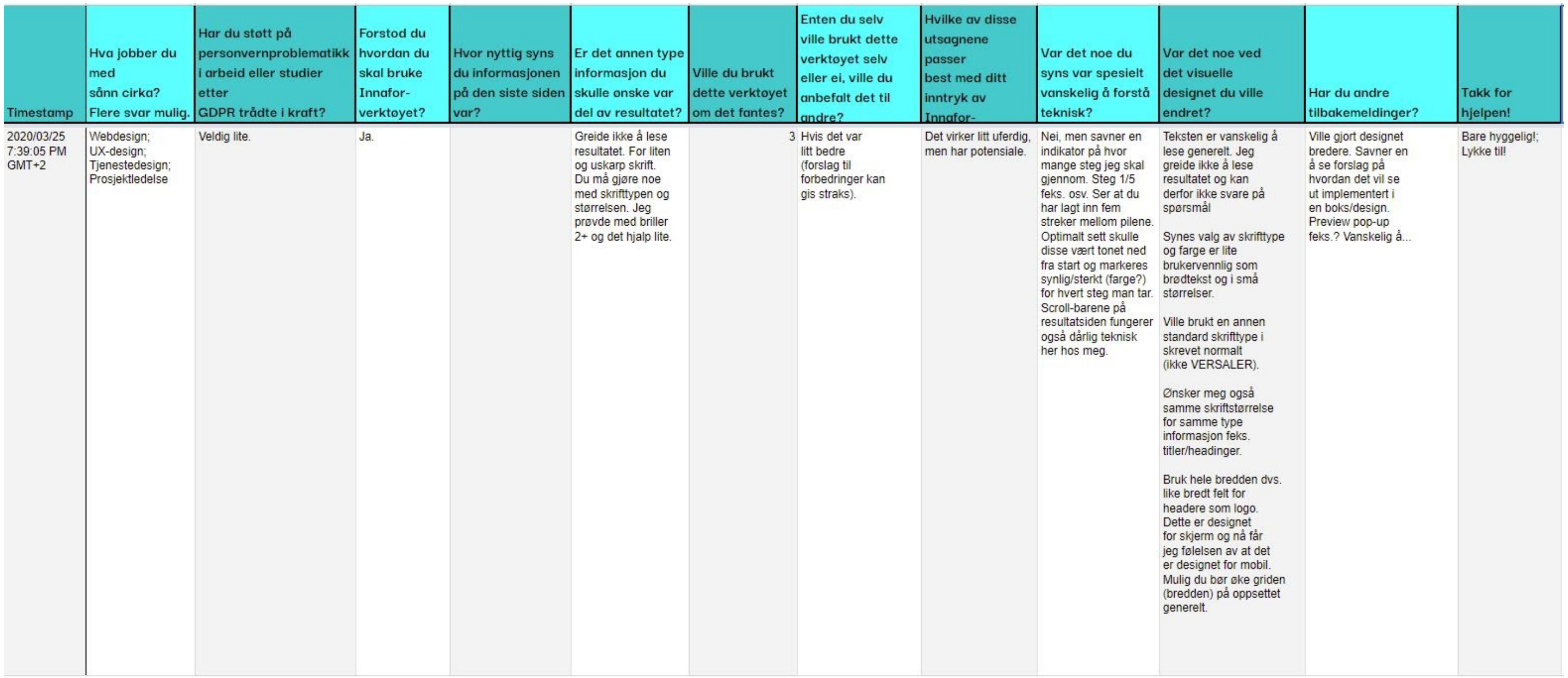
APPENDIX 7 – TEST RESULTS PHASE 1

10.7.1 Response nr 1 pt 1



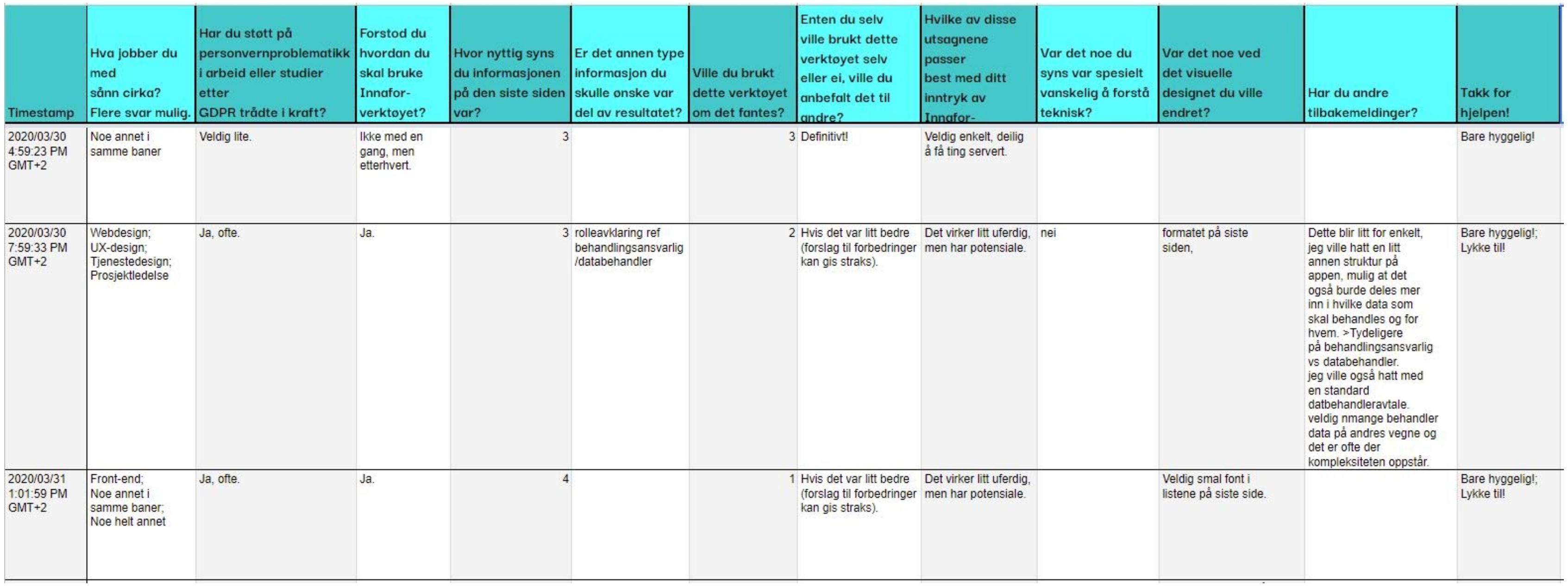
Timestamp	Hva jobber du med sånn cirka? Flere svar mulig.	Har du støtt på personvernproblematikk i arbeid eller studier etter GDPR trådte i kraft?	Forstod du hvordan du skal bruke Innafor-verktøyet?	Hvor nyttig syns du informasjonen på den siste siden var?	Er det annen type informasjon du skulle ønske var del av resultatet?	Ville du brukt dette verktøyet om det fantes?	Enten du selv ville brukt dette verktøyet selv eller ei, ville du anbefalt det til andre?	Hvilke av disse utsagnene passer best med ditt inntryk av Innafor-	Var det noe du syns var spesielt vanskelig å forstå teknisk?	Var det noe ved det visuelle designet du ville endret?	Har du andre tilbakemeldinger?	Takk for hjelpen!
2020/03/25 7:39:05 PM GMT+2	Webdesign; UX-design; Tjenestedesign; Prosjektledelse	Veldig lite.	Ja.		Greide ikke å lese resultatet. For liten og uskarp skrift. Du må gjøre noe med skrifttypen og størrelsen. Jeg prøvde med briller 2+ og det hjalp lite.	3	Hvis det var litt bedre (forslag til forbedringer kan gis straks).	Det virker litt uferdig, men har potensiale.	Nei, men savner en indikator på hvor mange steg jeg skal gjennom. Steg 1/5 feks. osv. Ser at du har lagt inn fem streker mellom pilene. Optimalt sett skulle disse vært tonet ned fra start og markeres synlig/sterkt (farge?) for hvert steg man tar. Scroll-barene på resultatsiden fungerer også dårlig teknisk her hos meg.	Teksten er vanskelig å lese generelt. Jeg greide ikke å lese resultatet og kan derfor ikke svare på spørsmål Synes valg av skrifttype og farge er lite brukervennlig som brødtekst og i små størrelser. Ville brukt en annen standard skrifttype i skrevet normalt (ikke VERSALER). Ønsker meg også samme skriftstørrelse for samme type informasjon feks. titler/headinger. Bruk hele bredden dvs. like bredt felt for headere som logo. Dette er designet for skjerm og nå får jeg følelsen av at det er designet for mobil. Mulig du bør øke griden (bredden) på oppsettet generelt.	Ville gjort designet bredere. Savner en å se forslag på hvordan det vil se ut implementert i en boks/design. Preview pop-up feks.? Vanskelig å...	Bare hyggelig!; Lykke til!

10.7.2 Response nr 1 pt 2



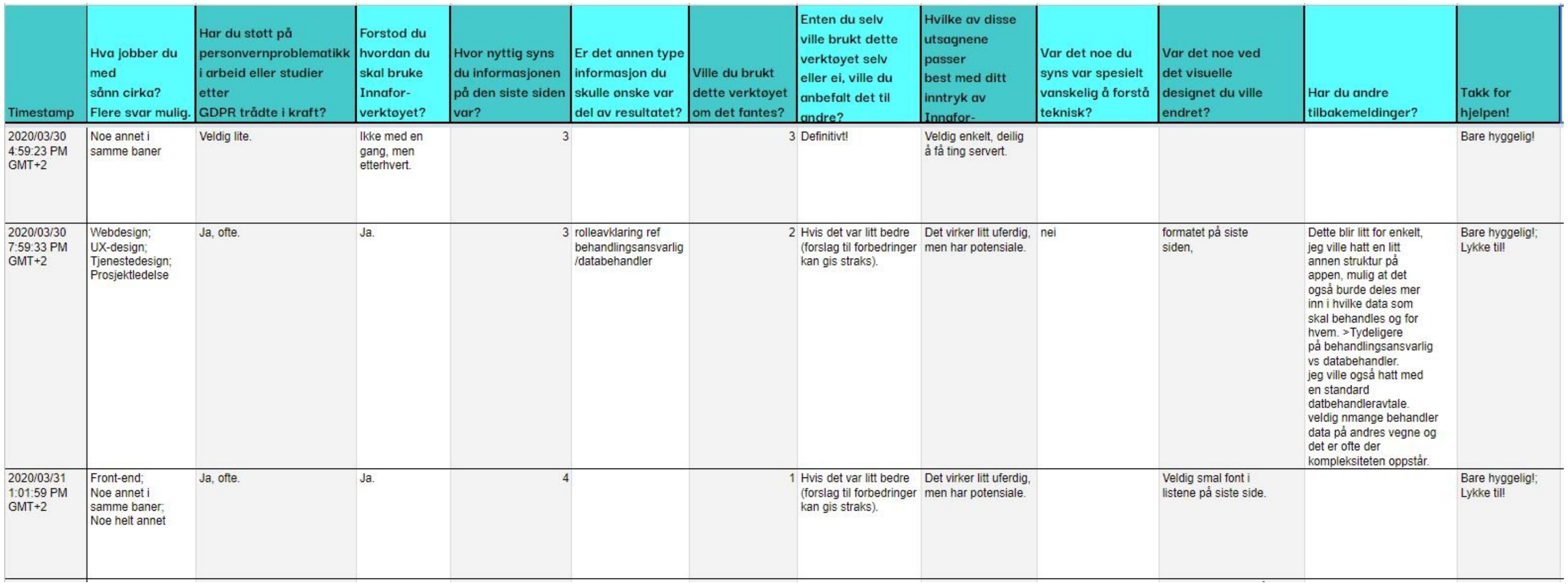
Timestamp	Hva jobber du med sånn cirka? Flere svar mulig.	Har du støtt på personvernproblematikk i arbeid eller studier etter GDPR trådte i kraft?	Forstod du hvordan du skal bruke Innafor-verktøyet?	Hvor nyttig syns du informasjonen på den siste siden var?	Er det annen type informasjon du skulle ønske var del av resultatet?	Ville du brukt dette verktøyet om det fantes?	Enten du selv ville brukt dette verktøyet selv eller ei, ville du anbefalt det til andre?	Hvilke av disse utsagnene passer best med ditt inntryk av Innafor-	Var det noe du syns var spesielt vanskelig å forstå teknisk?	Var det noe ved det visuelle designet du ville endret?	Har du andre tilbakemeldinger?	Takk for hjelpen!
2020/03/25 7:39:05 PM GMT+2	Webdesign; UX-design; Tjenestedesign; Prosjektledelse	Veldig lite.	Ja.		Greide ikke å lese resultatet. For liten og uskarp skrift. Du må gjøre noe med skrifttypen og størrelsen. Jeg prøvde med briller 2+ og det hjalp lite.	3	Hvis det var litt bedre (forslag til forbedringer kan gis straks).	Det virker litt uferdig, men har potensiale.	Nei, men savner en indikator på hvor mange steg jeg skal gjennom. Steg 1/5 feks. osv. Ser at du har lagt inn fem streker mellom pilene. Optimalt sett skulle disse vært tonet ned fra start og markeres synlig/sterkt (farge?) for hvert steg man tar. Scroll-barene på resultatsiden fungerer også dårlig teknisk her hos meg.	Teksten er vanskelig å lese generelt. Jeg greide ikke å lese resultatet og kan derfor ikke svare på spørsmål Synes valg av skrifttype og farge er lite brukervennlig som brødtekst og i små størrelser. Ville brukt en annen standard skrifttype i skrevet normalt (ikke VERSALER). Ønsker meg også samme skriftstørrelse for samme type informasjon feks. titler/headinger. Bruk hele bredden dvs. like bredt felt for headere som logo. Dette er designet for skjerm og nå får jeg følelsen av at det er designet for mobil. Mulig du bør øke griden (bredden) på oppsettet generelt.	Ville gjort designet bredere. Savner en å se forslag på hvordan det vil se ut implementert i en boks/design. Preview pop-up feks.? Vanskelig å...	Bare hyggelig!; Lykke til!

10.7.3 Response nr 2-4 pt 1



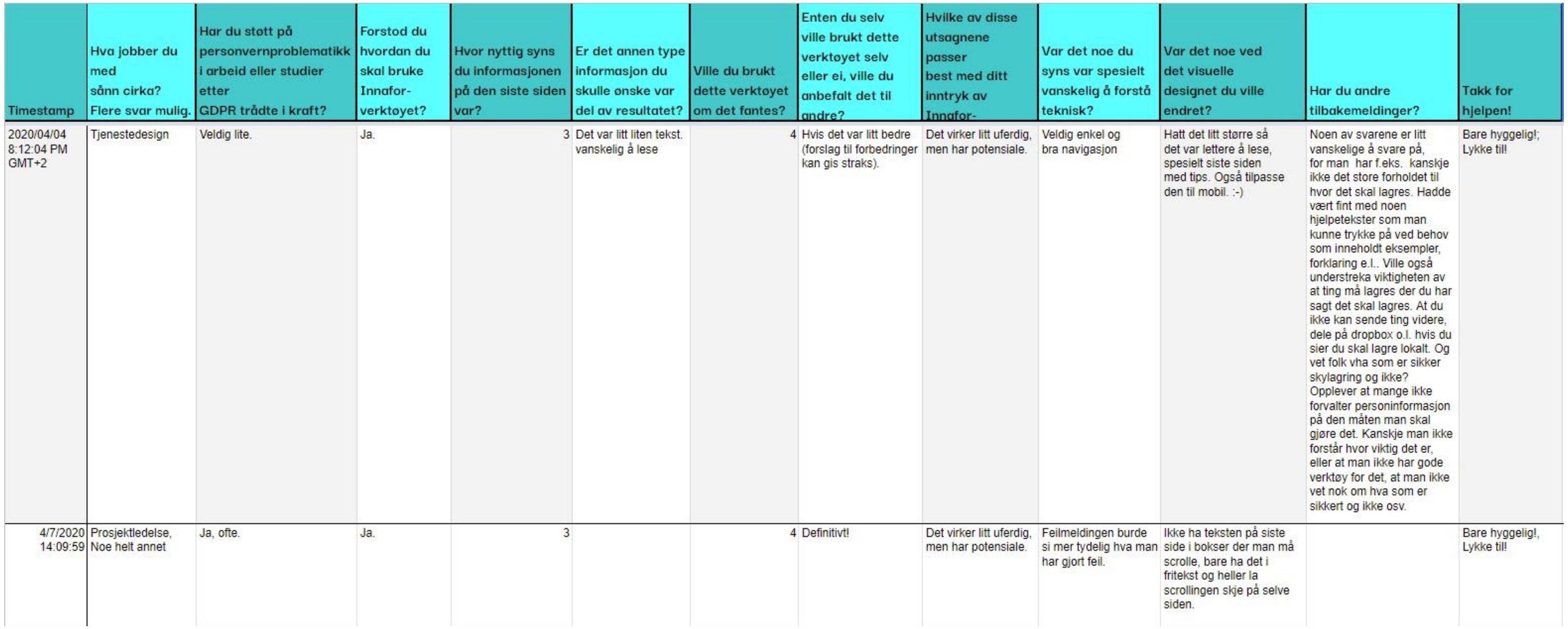
Timestamp	Hva jobber du med sånn cirka? Flere svar mulig.	Har du støtt på personvernproblematikk i arbeid eller studier etter GDPR trådte i kraft?	Forstod du hvordan du skal bruke Innafor-verktøyet?	Hvor nyttig syns du informasjonen på den siste siden var?	Er det annen type informasjon du skulle ønske var del av resultatet?	Ville du brukt dette verktøyet om det fantes?	Enten du selv ville brukt dette verktøyet selv eller ei, ville du anbefalt det til andre?	Hvilke av disse utsagnene passer best med ditt inntryk av Innafor-	Var det noe du syns var spesielt vanskelig å forstå teknisk?	Var det noe ved det visuelle designet du ville endret?	Har du andre tilbakemeldinger?	Takk for hjelpen!
2020/03/30 4:59:23 PM GMT+2	Noe annet i samme baner	Veldig lite.	Ikke med en gang, men etterhvert.	3		3	Definitivt!	Veldig enkelt, deilig å få ting servert.				Bare hyggelig!
2020/03/30 7:59:33 PM GMT+2	Webdesign; UX-design; Tjenestedesign; Prosjektledelse	Ja, ofte.	Ja.	3	rolleavklaring ref behandlingsansvarlig /databehandler	2	Hvis det var litt bedre (forslag til forbedringer kan gis straks).	Det virker litt uferdig, men har potensiale.	nei	formatet på siste siden,	Dette blir litt for enkelt, jeg ville hatt en litt annen struktur på appen, mulig at det også burde deles mer inn i hvilke data som skal behandles og for hvem. >Tydeligere på behandlingsansvarlig vs databehandler. jeg ville også hatt med en standard datbehandleravtale. veldig nmange behandler data på andres vegne og det er ofte der kompleksiteten oppstår.	Bare hyggelig!; Lykke til!
2020/03/31 1:01:59 PM GMT+2	Front-end; Noe annet i samme baner; Noe helt annet	Ja, ofte.	Ja.	4		1	Hvis det var litt bedre (forslag til forbedringer kan gis straks).	Det virker litt uferdig, men har potensiale.		Veldig smal font i listene på siste side.		Bare hyggelig!; Lykke til!

10.7.4 Response nr 2-4 pt 2



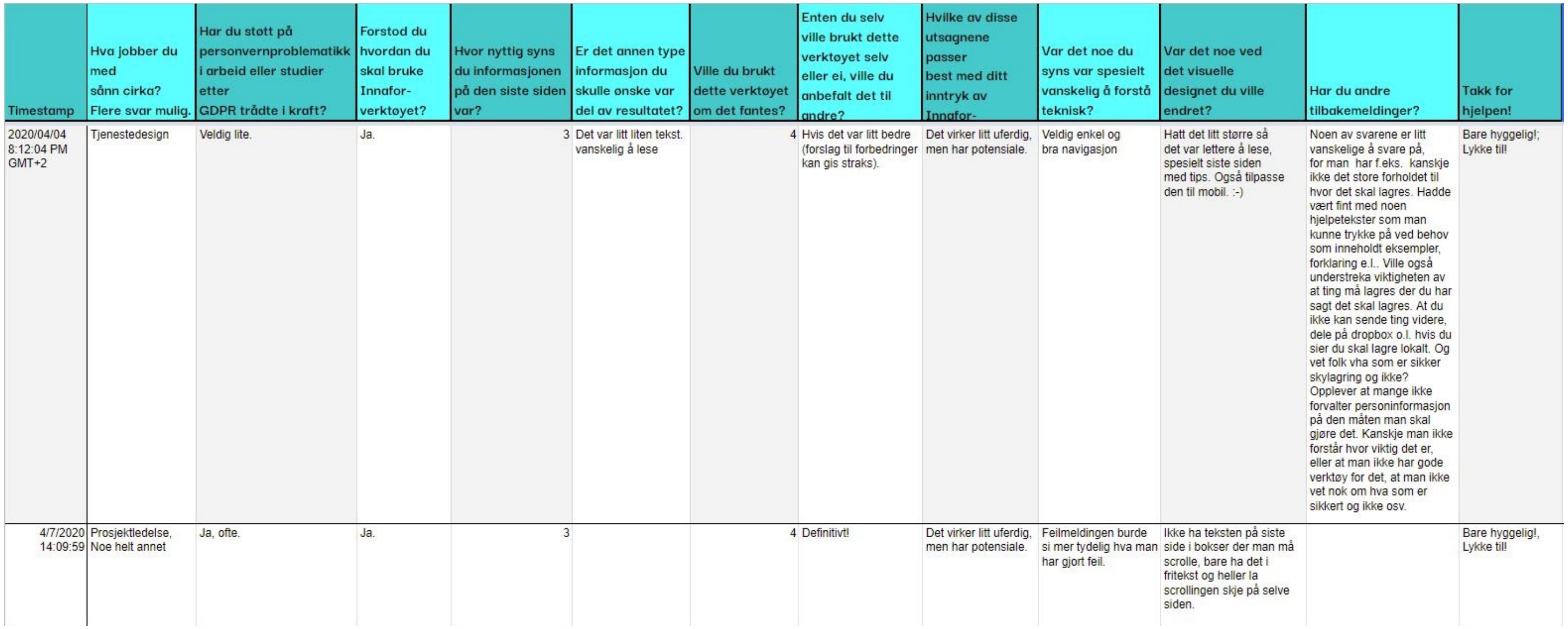
Timestamp	Hva jobber du med sånn cirka? Flere svar mulig.	Har du støtt på personvernproblematikk i arbeid eller studier etter GDPR trådte i kraft?	Forstod du hvordan du skal bruke Innafor-verktøyet?	Hvor nyttig syns du informasjonen på den siste siden var?	Er det annen type informasjon du skulle ønske var del av resultatet?	Ville du brukt dette verktøyet om det fantes?	Enten du selv ville brukt dette verktøyet selv eller ei, ville du anbefalt det til andre?	Hvilke av disse utsagnene passer best med ditt inntryk av Innafor-	Var det noe du syns var spesielt vanskelig å forstå teknisk?	Var det noe ved det visuelle designet du ville endret?	Har du andre tilbakemeldinger?	Takk for hjelpen!
2020/03/30 4:59:23 PM GMT+2	Noe annet i samme baner	Veldig lite.	Ikke med en gang, men etterhvert.	3		3	Definitivt!	Veldig enkelt, deilig å få ting servert.				Bare hyggelig!
2020/03/30 7:59:33 PM GMT+2	Webdesign; UX-design; Tjenestedesign; Prosjektledelse	Ja, ofte.	Ja.	3	rolleavklaring ref behandlingsansvarlig /databehandler	2	Hvis det var litt bedre (forslag til forbedringer kan gis straks).	Det virker litt uferdig, men har potensiale.	nei	formatet på siste siden,	Dette blir litt for enkelt, jeg ville hatt en litt annen struktur på appen, mulig at det også burde deles mer inn i hvilke data som skal behandles og for hvem. >Tydeligere på behandlingsansvarlig vs databehandler. jeg ville også hatt med en standard datbehandleravtale. veldig nmange behandler data på andres vegne og det er ofte der kompleksiteten oppstår.	Bare hyggelig!; Lykke til!
2020/03/31 1:01:59 PM GMT+2	Front-end; Noe annet i samme baner; Noe helt annet	Ja, ofte.	Ja.	4		1	Hvis det var litt bedre (forslag til forbedringer kan gis straks).	Det virker litt uferdig, men har potensiale.		Veldig smal font i listene på siste side.		Bare hyggelig!; Lykke til!

10.7.5 Response nr 5-6 pt 1



Timestamp	Hva jobber du med sånn cirka? Flere svar mulig.	Har du støtt på personvernproblematikk i arbeid eller studier etter GDPR trådte i kraft?	Forstod du hvordan du skal bruke Innafor-verktøyet?	Hvor nyttig syns du informasjonen på den siste siden var?	Er det annen type informasjon du skulle ønske var del av resultatet?	Ville du brukt dette verktøyet om det fantes?	Enten du selv ville brukt dette verktøyet selv eller ei, ville du anbefalt det til andre?	Hvilke av disse utsagnene passer best med ditt inntryk av Innafor-	Var det noe du syns var spesielt vanskelig å forstå teknisk?	Var det noe ved det visuelle designet du ville endret?	Har du andre tilbakemeldinger?	Takk for hjelpen!
2020/04/04 8:12:04 PM GMT+2	Tjenestedesign	Veldig lite.	Ja.	3	Det var litt liten tekst. vanskelig å lese	4	Hvis det var litt bedre (forslag til forbedringer kan gis straks).	Det virker litt uferdig, men har potensiale.	Veldig enkel og bra navigasjon	Hatt det litt større så det var lettere å lese, spesielt siste siden med tips. Også tilpasse den til mobil. :-)	Noen av svarene er litt vanskelige å svare på, for man har f.eks. kanskje ikke det store forholdet til hvor det skal lagres. Hadde vært fint med noen hjelpetekster som man kunne trykke på ved behov som inneholdt eksempler, forklaring e.l.. Ville også understreka viktigheten av at ting må lagres der du har sagt det skal lagres. At du ikke kan sende ting videre, dele på dropbox o.l. hvis du sier du skal lagre lokalt. Og vet folk vha som er sikker skylagring og ikke? Opplever at mange ikke forvalter personinformasjon på den måten man skal gjøre det. Kanskje man ikke forstår hvor viktig det er, eller at man ikke har gode verktøy for det, at man ikke vet nok om hva som er sikkert og ikke osv.	Bare hyggelig!; Lykke til!
4/7/2020 14:09:59	Prosjektledelse, Noe helt annet	Ja, ofte.	Ja.	3		4	Definitivt!	Det virker litt uferdig, men har potensiale.	Feilmeldingen burde si mer tydelig hva man har gjort feil.	Ikke ha teksten på siste side i bokser der man må scrolle, bare ha det i fritekst og heller la scrollingen skje på selve siden.		Bare hyggelig!, Lykke til!

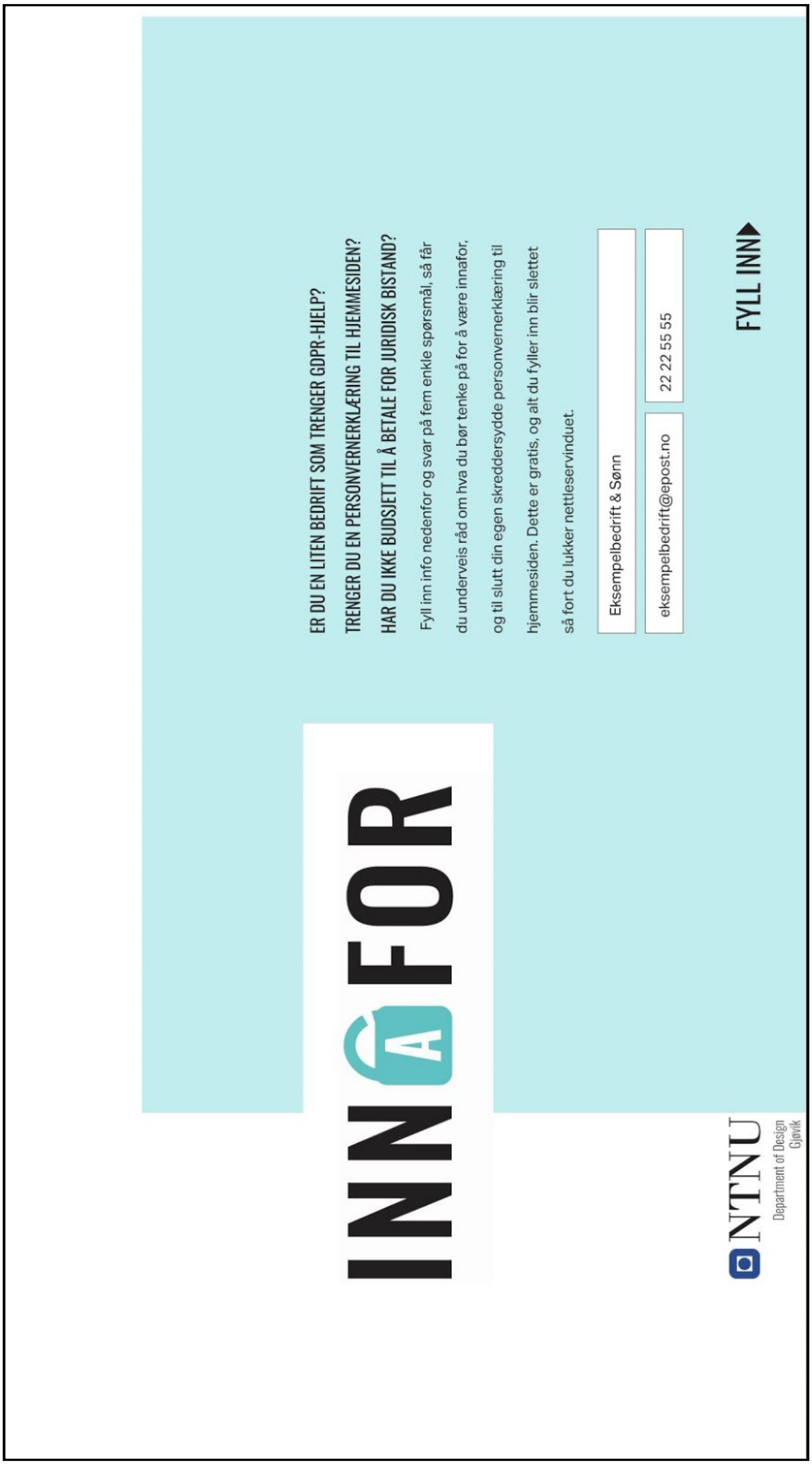
10.7.6 Response nr 5-6 pt 2



Timestamp	Hva jobber du med sånn cirka? Flere svar mulig.	Har du støtt på personvernproblematikk i arbeid eller studier etter GDPR trådte i kraft?	Forstod du hvordan du skal bruke Innafor-verktøyet?	Hvor nyttig syns du informasjonen på den siste siden var?	Er det annen type informasjon du skulle ønske var del av resultatet?	Ville du brukt dette verktøyet om det fantes?	Enten du selv ville brukt dette verktøyet selv eller ei, ville du anbefalt det til andre?	Hvilke av disse utsagnene passer best med ditt inntryk av Innafor-	Var det noe du syns var spesielt vanskelig å forstå teknisk?	Var det noe ved det visuelle designet du ville endret?	Har du andre tilbakemeldinger?	Takk for hjelpen!
2020/04/04 8:12:04 PM GMT+2	Tjenestedesign	Veldig lite.	Ja.	3	Det var litt liten tekst. vanskelig å lese	4	Hvis det var litt bedre (forslag til forbedringer kan gis straks).	Det virker litt uferdig, men har potensiale.	Veldig enkel og bra navigasjon	Hatt det litt større så det var lettere å lese, spesielt siste siden med tips. Også tilpasse den til mobil. :-)	Noen av svarene er litt vanskelige å svare på, for man har f.eks. kanskje ikke det store forholdet til hvor det skal lagres. Hadde vært fint med noen hjelpetekster som man kunne trykke på ved behov som inneholdt eksempler, forklaring e.l.. Ville også understreka viktigheten av at ting må lagres der du har sagt det skal lagres. At du ikke kan sende ting videre, dele på dropbox o.l. hvis du sier du skal lagre lokalt. Og vet folk vha som er sikker skylagring og ikke? Opplever at mange ikke forvalter personinformasjon på den måten man skal gjøre det. Kanskje man ikke forstår hvor viktig det er, eller at man ikke har gode verktøy for det, at man ikke vet nok om hva som er sikkert og ikke osv.	Bare hyggelig!; Lykke til!
4/7/2020 14:09:59	Prosjektledelse, Noe helt annet	Ja, ofte.	Ja.	3		4	Definitivt!	Det virker litt uferdig, men har potensiale.	Feilmeldingen burde si mer tydelig hva man har gjort feil.	Ikke ha teksten på siste side i bokser der man må scrolle, bare ha det i fritekst og heller la scrollingen skje på selve siden.		Bare hyggelig!, Lykke til!

APPENDIX 8 - THE FINAL PROTOTYPE

10.8.1 Final first page



ER DU EN LITEN BEDRIFT SOM TRENGER GDPR-HJELP?

TRENGER DU EN PERSONVERNERKLÆRING TIL HJEMMESIDEN?

HAR DU IKKE BUDSJETT TIL Å BETALE FOR JURIDISK BISTAND?

Fyll inn info nedenfor og svar på fem enkle spørsmål, så får du underveis råd om hva du bør tenke på for å være innafor, og til slutt din egen skreddersydde personvernerklæring til hjemmesiden. Dette er gratis, og alt du fyller inn blir slettet så fort du lukker nettleservinduet.

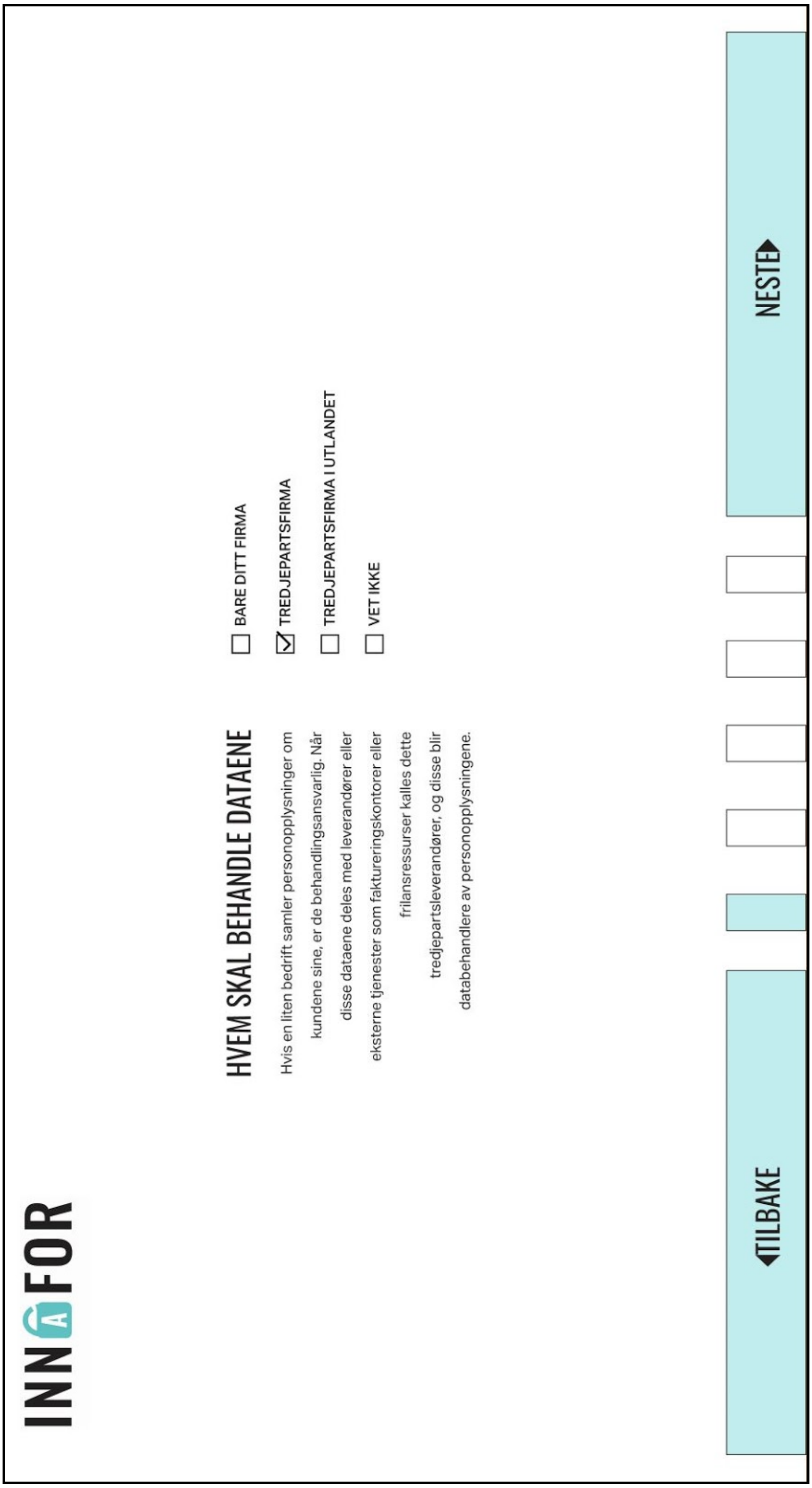
Eksempelbedrift & Sønn

eksempelbedrift@epost.no

22 22 55 55

FYLL INN▶

10.8.2 WHO (Hvem) checkbox page

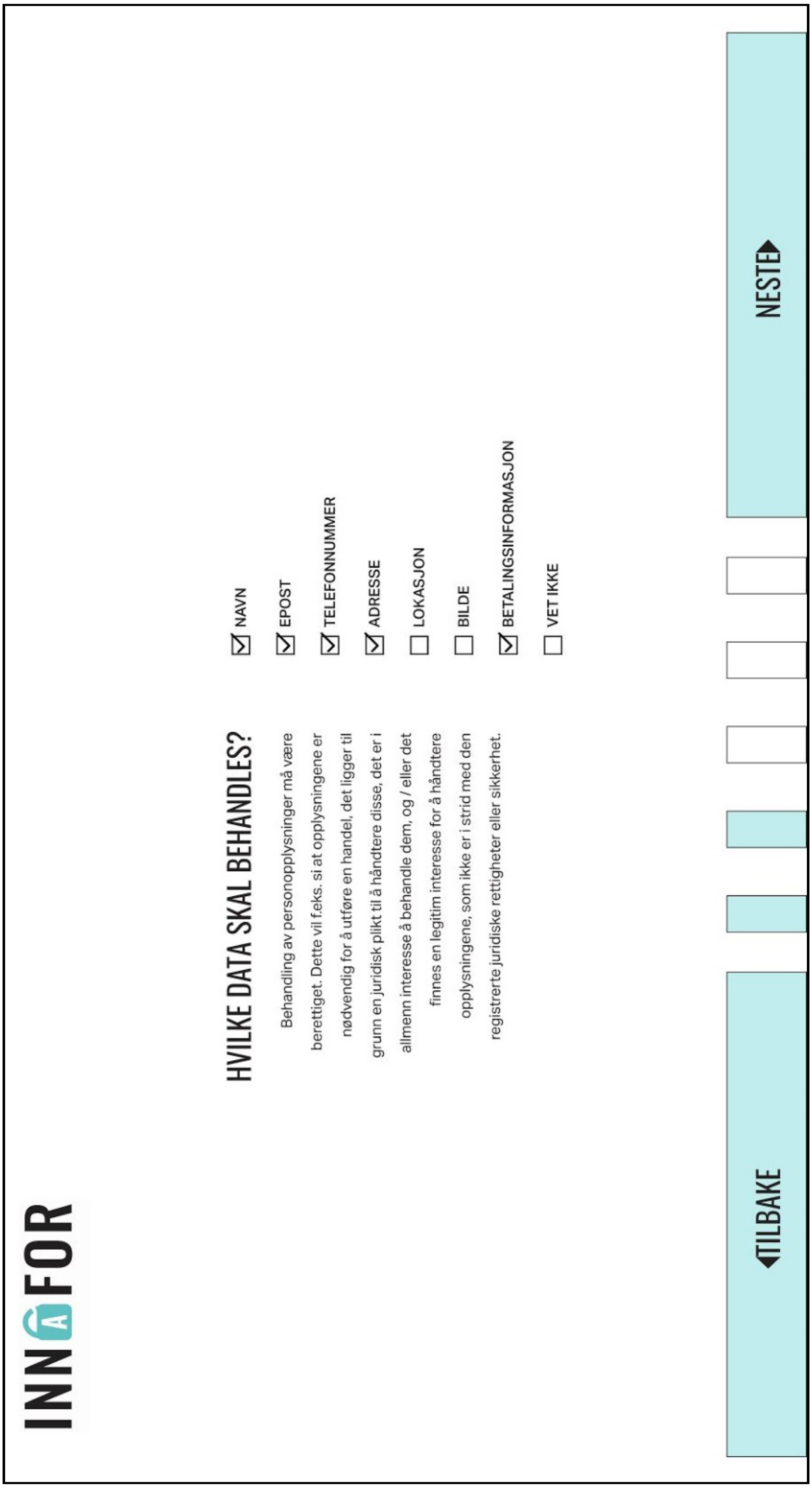


HVEM SKAL BEHANDLE DATAENE

Hvis en liten bedrift samler personopplysninger om kundene sine, er de behandlingsansvarlig. Når disse dataene deles med leverandører eller eksterne tjenester som faktureringskontorer eller frilansressurser kalles dette tredjepartsleverandører, og disse blir databehandlere av personopplysningene.

□ BARE DITT FIRMA
☑ TREDJEPARTSFIRMA
□ TREDJEPARTSFIRMA I UTLANDET
□ VET IKKE

10.8.3 WHAT (Hvilke) checkbox page

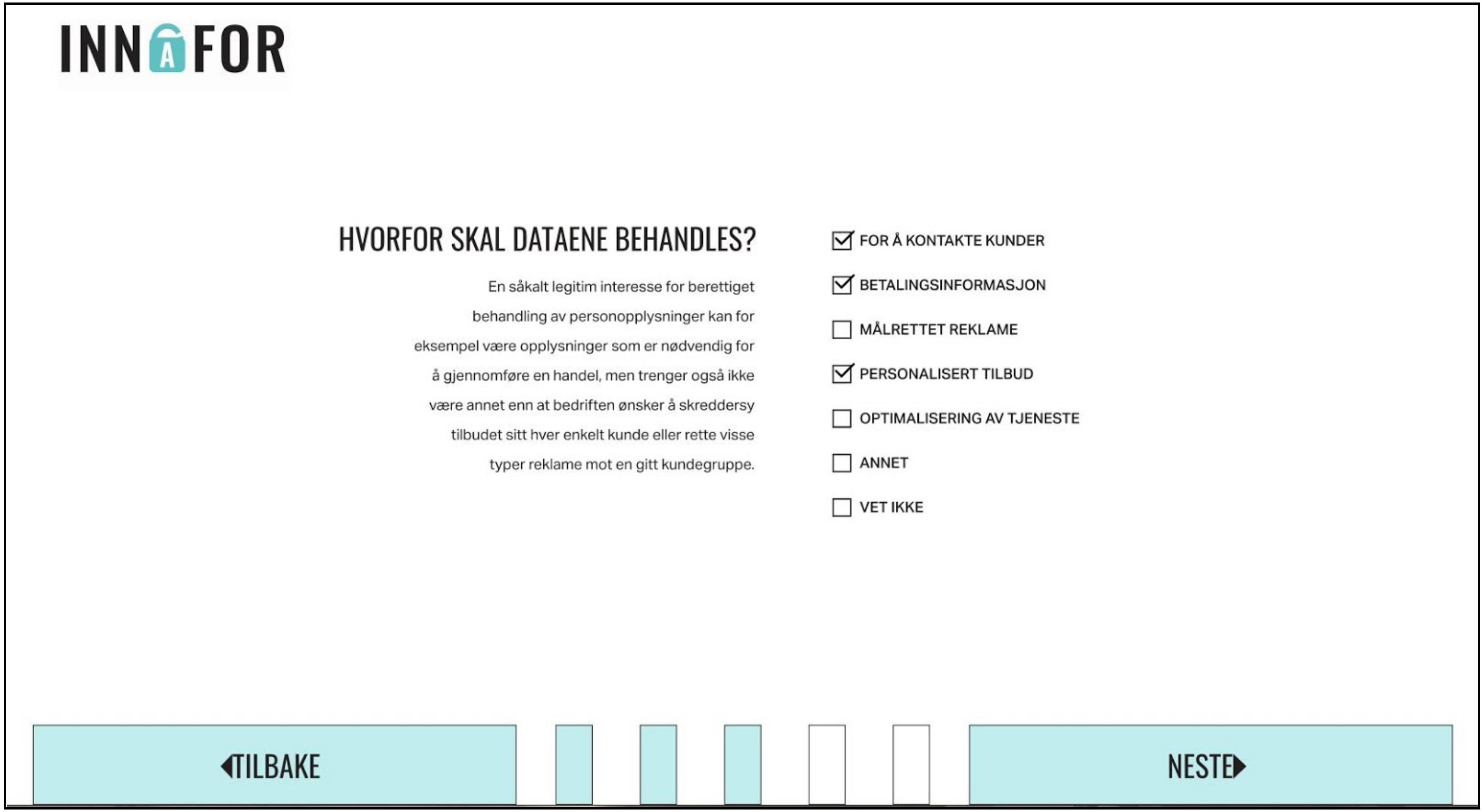


HVILKE DATA SKAL BEHANDLES?

Behandling av personopplysninger må være berettiget. Dette vil f.eks. si at opplysningene er nødvendig for å utføre en handel, det ligger til grunn en juridisk plikt til å håndtere disse, det er i allmenn interesse å behandle dem, og / eller det finnes en legitim interesse for å håndtere opplysningene, som ikke er i strid med den registrerte juridiske rettigheter eller sikkerhet.

☑ NAVN
☑ EPOST
☑ TELEFONNUMMER
☑ ADRESSE
□ LOKASJON
□ BILDE
☑ BETALINGSINFORMASJON
□ VET IKKE

10.8.4 WHY (Hvorfor) checkbox page

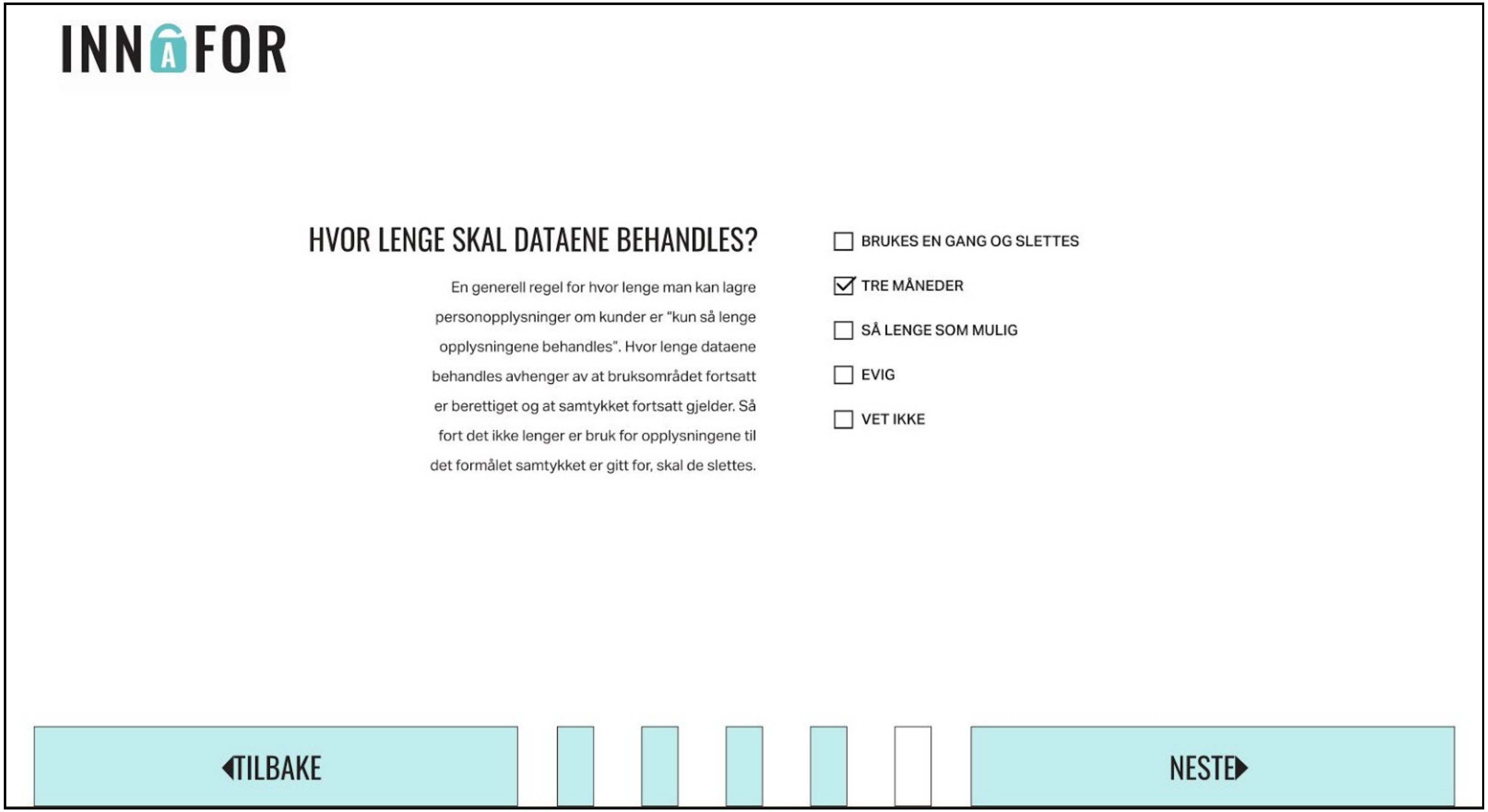


HVORFOR SKAL DATAENE BEHANDLES?

En såkalt legitim interesse for berettiget behandling av personopplysninger kan for eksempel være opplysninger som er nødvendig for å gjennomføre en handel, men trenger også ikke være annet enn at bedriften ønsker å skreddersy tilbudet sitt hver enkelt kunde eller rette visse typer reklame mot en gitt kundegruppe.

- ☑ FOR Å KONTAKTE KUNDER
- ☑ BETALINGSINFORMASJON
- □ MÅLRETTET REKLAME
- ☑ PERSONALISERT TILBUD
- □ OPTIMALISERING AV TJENESTE
- □ ANNET
- □ VET IKKE

10.8.5 HOW LONG (Hvor lenge) checkbox page



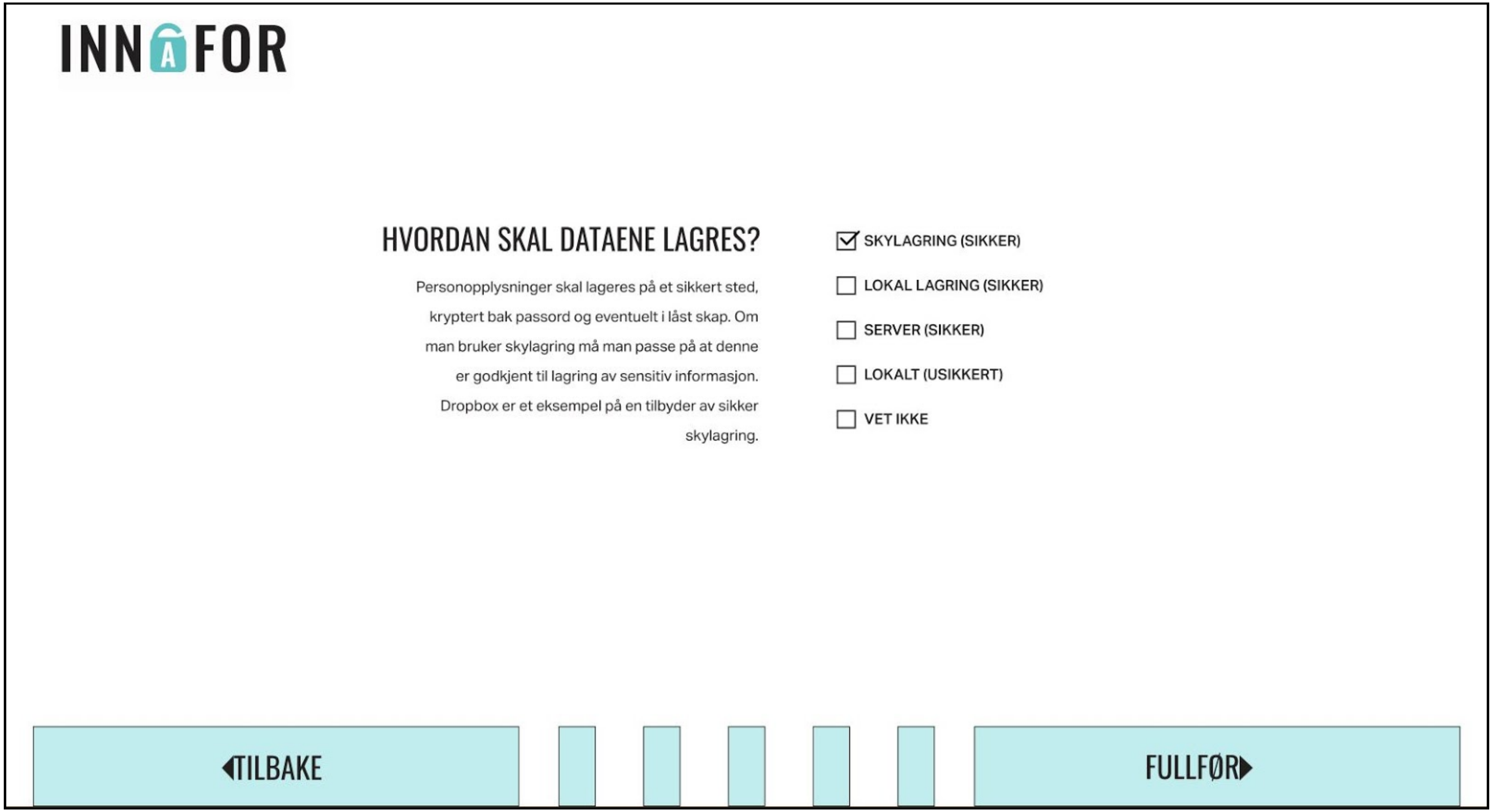
INNÅFOR

HVOR LENGE SKAL DATAENE BEHANDLES?

En generell regel for hvor lenge man kan lagre personopplysninger om kunder er "kun så lenge opplysningene behandles". Hvor lenge dataene behandles avhenger av at bruksområdet fortsatt er berettiget og at samtykket fortsatt gjelder. Så fort det ikke lenger er bruk for opplysningene til det formålet samtykket er gitt for, skal de slettes.

☐ BRUKES EN GANG OG SLETTES
☑ TRE MÅNEDER
☐ SÅ LENGE SOM MULIG
☐ EVIG
☐ VET IKKE

10.8.5 HOW (Hvordan) checkbox page



HVORDAN SKAL DATAENE LAGRES?

Personopplysninger skal lageres på et sikkert sted, kryptert bak passord og eventuelt i låst skap. Om man bruker skylagring må man passe på at denne er godkjent til lagring av sensitiv informasjon. Dropbox er et eksempel på en tilbyder av sikker skylagring.

☑ SKYLAGRING (SIKKER)

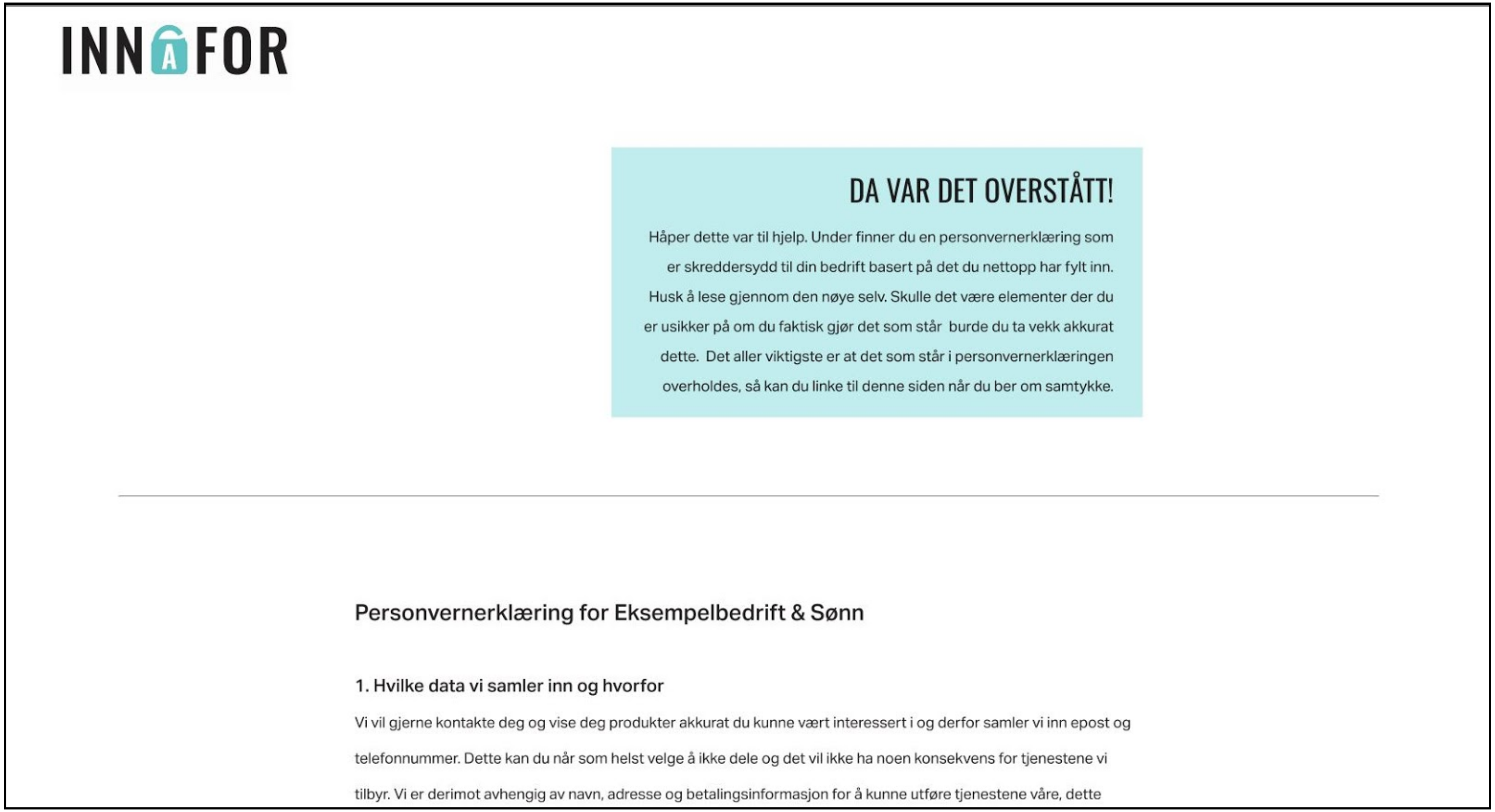
□ LOKAL LAGRING (SIKKER)

□ SERVER (SIKKER)

□ LOKALT (USIKKERT)

□ VET IKKE

10.8.6 Final result page pt 1 - Tailored



INNÅFOR

DA VAR DET OVERSTÅTT!

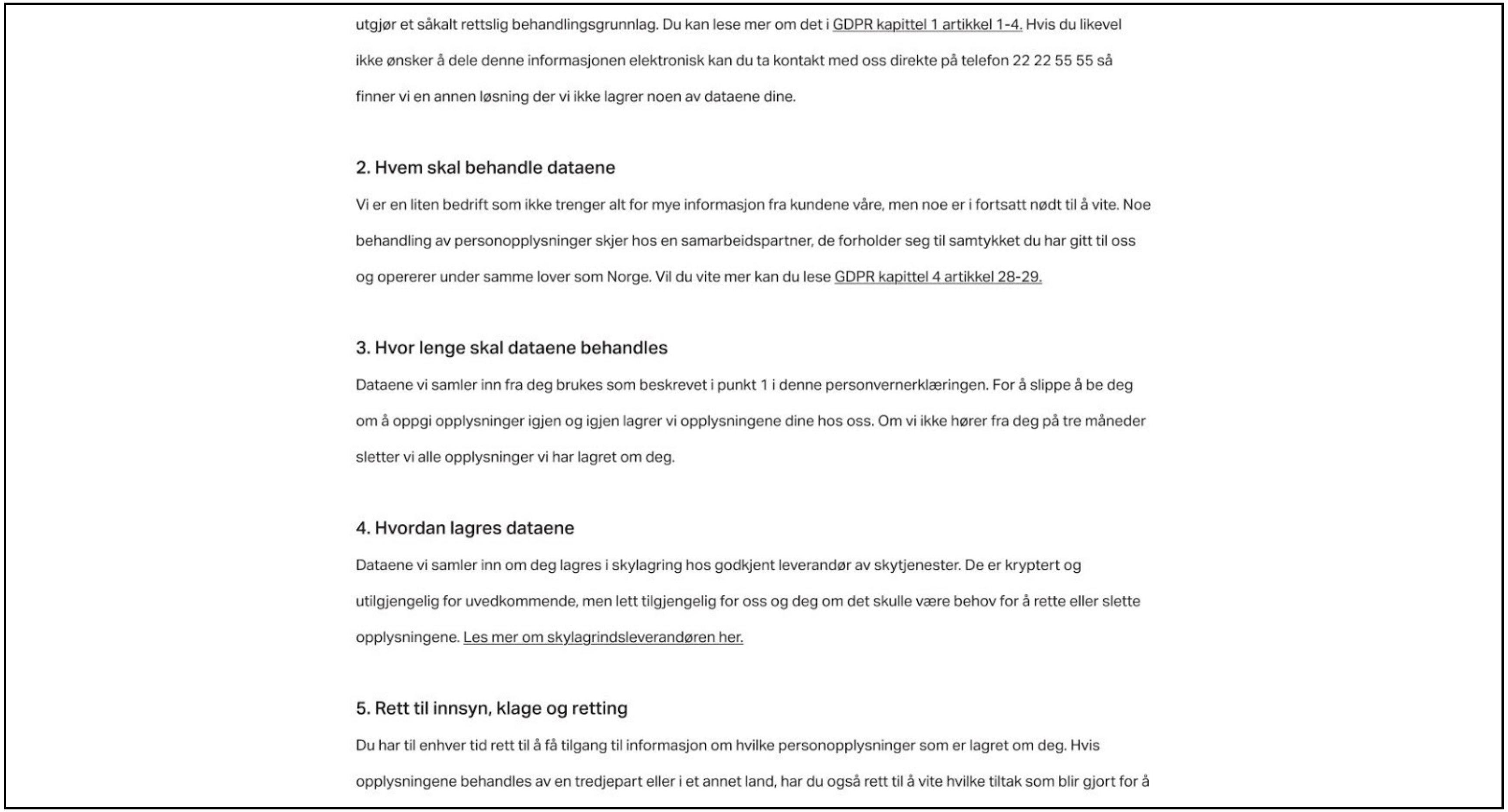
Håper dette var til hjelp. Under finner du en personvernerklæring som er skreddersydd til din bedrift basert på det du nettopp har fylt inn. Husk å lese gjennom den nøye selv. Skulle det være elementer der du er usikker på om du faktisk gjør det som står burde du ta vekk akkurat dette. Det aller viktigste er at det som står i personvernerklæringen overholdes, så kan du linke til denne siden når du ber om samtykke.

Personvernerklæring for Eksempelbedrift & Sønn

1. Hvilke data vi samler inn og hvorfor

Vi vil gjerne kontakte deg og vise deg produkter akkurat du kunne vært interessert i og derfor samler vi inn epost og telefonnummer. Dette kan du når som helst velge å ikke dele og det vil ikke ha noen konsekvens for tjenestene vi tilbyr. Vi er derimot avhengig av navn, adresse og betalingsinformasjon for å kunne utføre tjenestene våre, dette

10.8.7 Final result page pt 2 - Tailored



utgjør et såkalt rettslig behandlingsgrunnlag. Du kan lese mer om det i GDPR kapittel 1 artikkel 1-4. Hvis du likevel ikke ønsker å dele denne informasjonen elektronisk kan du ta kontakt med oss direkte på telefon 22 22 55 55 så finner vi en annen løsning der vi ikke lagrer noen av dataene dine.

2. Hvem skal behandle dataene

Vi er en liten bedrift som ikke trenger alt for mye informasjon fra kundene våre, men noe er i fortsatt nødt til å vite. Noe behandling av personopplysninger skjer hos en samarbeidspartner, de forholder seg til samtykket du har gitt til oss og opererer under samme lover som Norge. Vil du vite mer kan du lese GDPR kapittel 4 artikkel 28-29.

3. Hvor lenge skal dataene behandles

Dataene vi samler inn fra deg brukes som beskrevet i punkt 1 i denne personvernerklæringen. For å slippe å be deg om å oppgi opplysninger igjen og igjen lagrer vi opplysningene dine hos oss. Om vi ikke hører fra deg på tre måneder sletter vi alle opplysninger vi har lagret om deg.

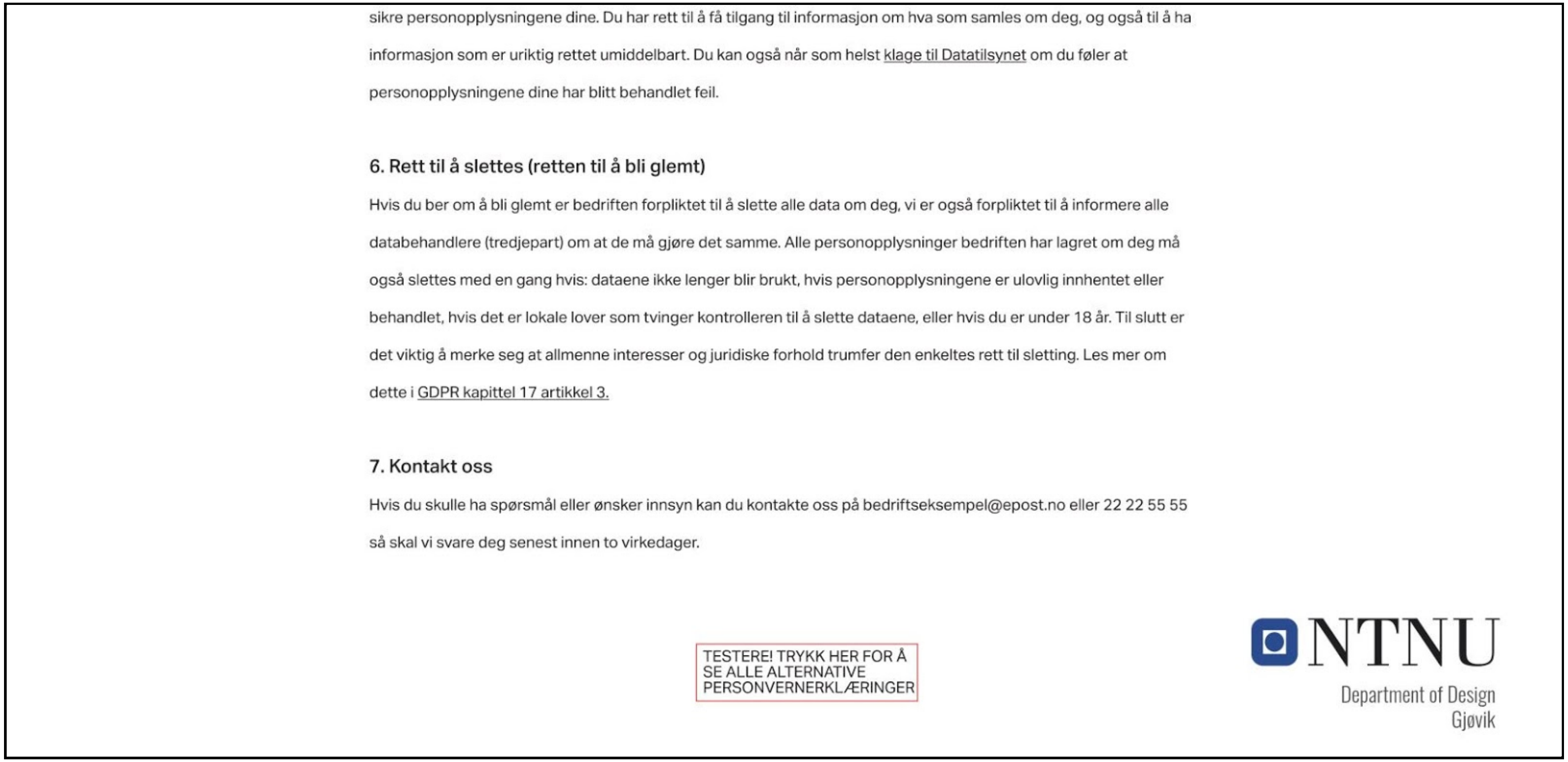
4. Hvordan lagres dataene

Dataene vi samler inn om deg lagres i skylagring hos godkjent leverandør av skytjenester. De er kryptert og utilgjengelig for uvedkommende, men lett tilgjengelig for oss og deg om det skulle være behov for å rette eller slette opplysningene. Les mer om skylagrindsleverandøren her.

5. Rett til innsyn, klage og retting

Du har til enhver tid rett til å få tilgang til informasjon om hvilke personopplysninger som er lagret om deg. Hvis opplysningene behandles av en tredjepart eller i et annet land, har du også rett til å vite hvilke tiltak som blir gjort for å

10.8.8 Final result page pt 3 - Tailored



sikre personopplysningene dine. Du har rett til å få tilgang til informasjon om hva som samles om deg, og også til å ha informasjon som er uriktig rettet umiddelbart. Du kan også når som helst klage til Datatilsynet om du føler at personopplysningene dine har blitt behandlet feil.

6. Rett til å slettes (retten til å bli glemt)

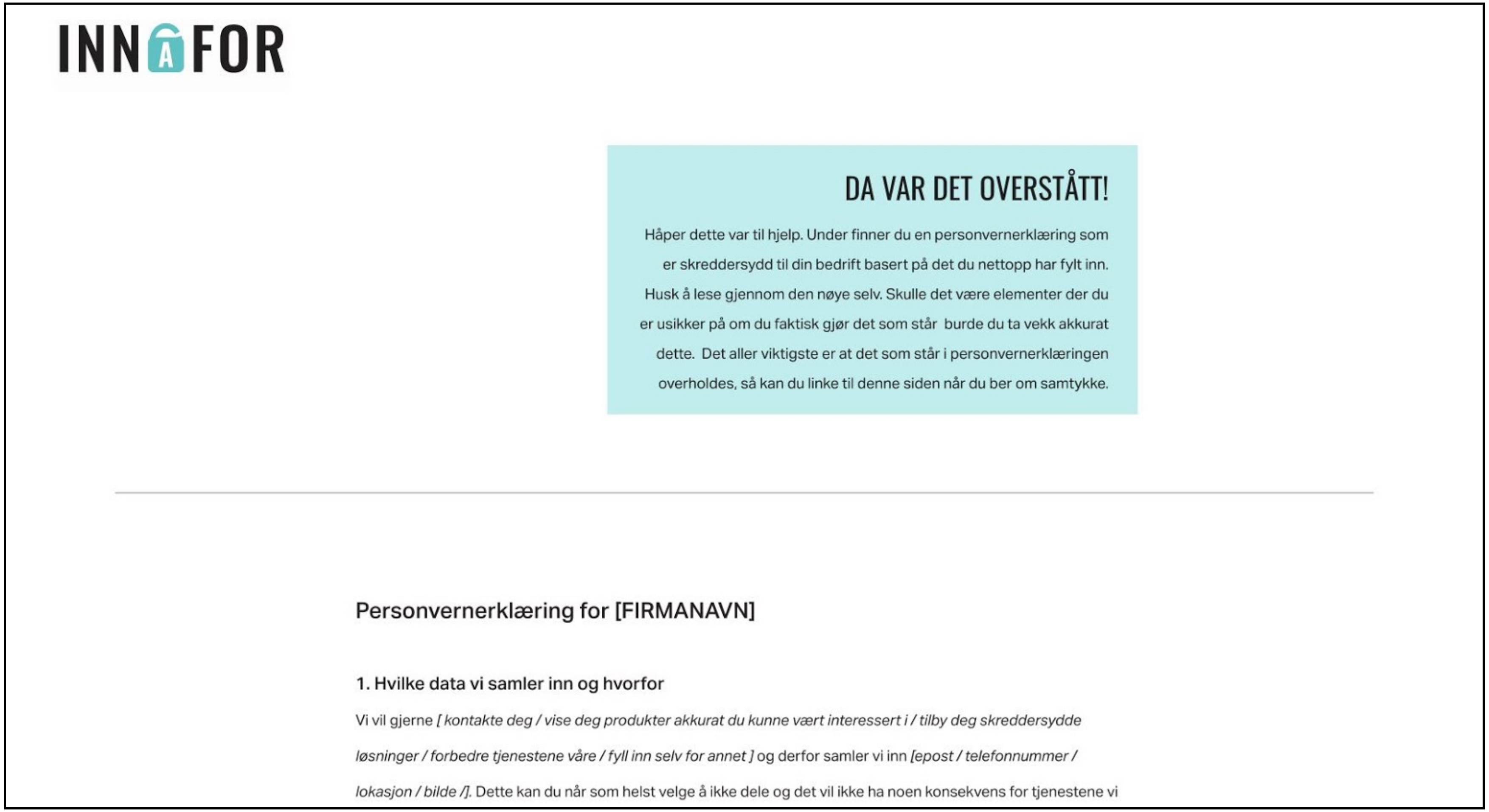
Hvis du ber om å bli glemt er bedriften forpliktet til å slette alle data om deg, vi er også forpliktet til å informere alle databehandlere (tredjepart) om at de må gjøre det samme. Alle personopplysninger bedriften har lagret om deg må også slettes med en gang hvis: dataene ikke lenger blir brukt, hvis personopplysningene er ulovlig innhentet eller behandlet, hvis det er lokale lover som tvinger kontrolleren til å slette dataene, eller hvis du er under 18 år. Til slutt er det viktig å merke seg at allmenne interesser og juridiske forhold trumfer den enkeltes rett til sletting. Les mer om dette i GDPR kapittel 17 artikkel 3.

7. Kontakt oss

Hvis du skulle ha spørsmål eller ønsker innsyn kan du kontakte oss på bedriftseksempel@epost.no eller 22 22 55 55 så skal vi svare deg senest innen to virkedager.

TESTERE! TRYKK HER FOR Å SE ALLE ALTERNATIVE PERSONVERNERKLÆRINGER

10.8.9 Final result page pt 1 - Untailored



INNÅFOR

DA VAR DET OVERSTÅTT!

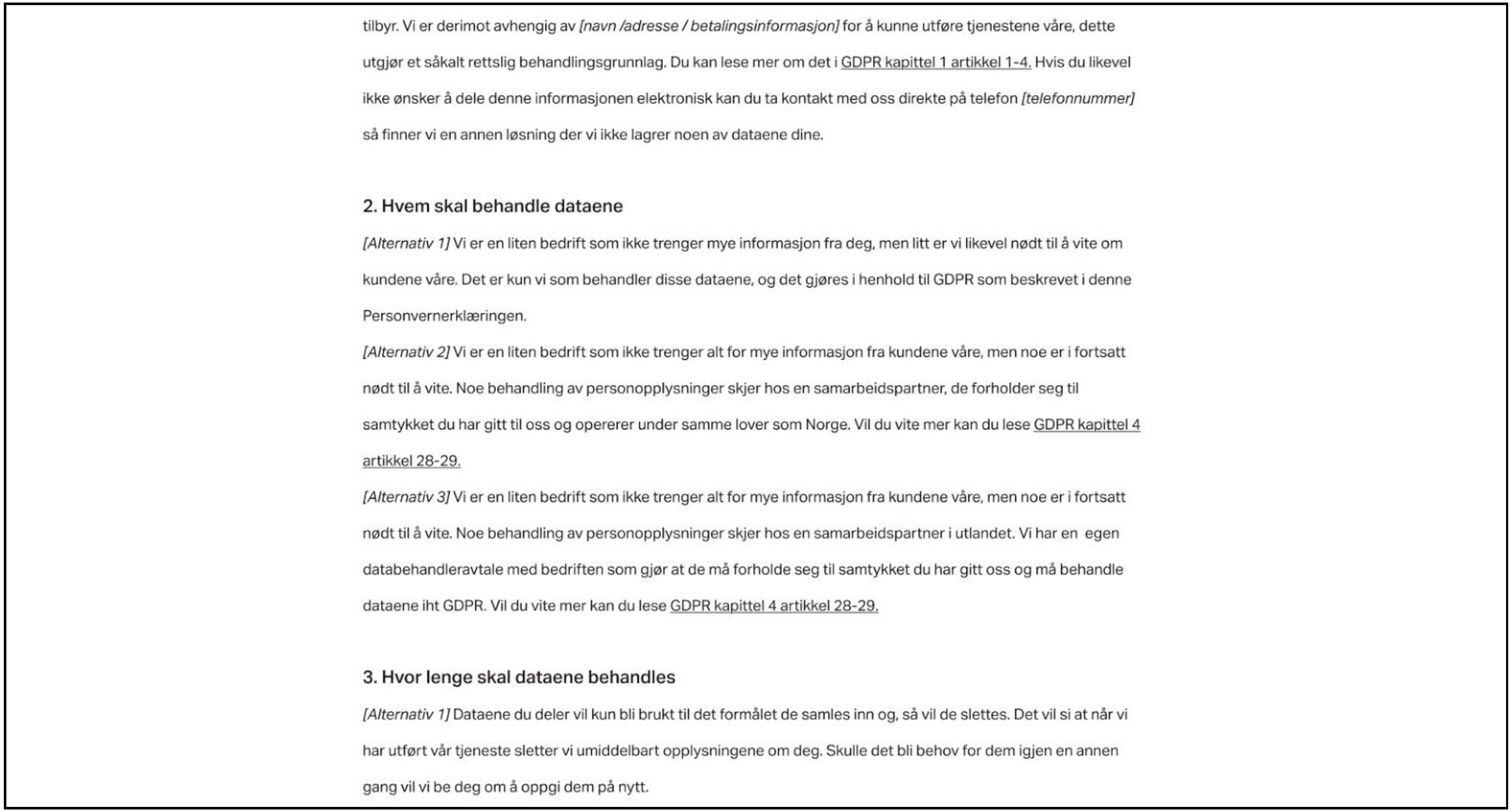
Håper dette var til hjelp. Under finner du en personvernerklæring som er skreddersydd til din bedrift basert på det du nettopp har fylt inn. Husk å lese gjennom den nøye selv. Skulle det være elementer der du er usikker på om du faktisk gjør det som står burde du ta vekk akkurat dette. Det aller viktigste er at det som står i personvernerklæringen overholdes, så kan du linke til denne siden når du ber om samtykke.

Personvernerklæring for [FIRMANAVN]

1. Hvilke data vi samler inn og hvorfor

Vi vil gjerne *[kontakte deg / vise deg produkter akkurat du kunne vært interessert i / tilby deg skreddersydde løsninger / forbedre tjenestene våre / fyll inn selv for annet]* og derfor samler vi inn *[epost / telefonnummer / lokasjon / bilde /]*. Dette kan du når som helst velge å ikke dele og det vil ikke ha noen konsekvens for tjenestene vi

10.8.10 Final result page pt 2 - Untailored



tilbyr. Vi er derimot avhengig av *[navn /adresse / betalingsinformasjon]* for å kunne utføre tjenestene våre, dette utgjør et såkalt rettslig behandlingsgrunnlag. Du kan lese mer om det i GDPR kapittel 1 artikkel 1-4. Hvis du likevel ikke ønsker å dele denne informasjonen elektronisk kan du ta kontakt med oss direkte på telefon *[telefonnummer]* så finner vi en annen løsning der vi ikke lagrer noen av dataene dine.

2. Hvem skal behandle dataene

[Alternativ 1] Vi er en liten bedrift som ikke trenger mye informasjon fra deg, men litt er vi likevel nødt til å vite om kundene våre. Det er kun vi som behandler disse dataene, og det gjøres i henhold til GDPR som beskrevet i denne Personvernerklæringen.

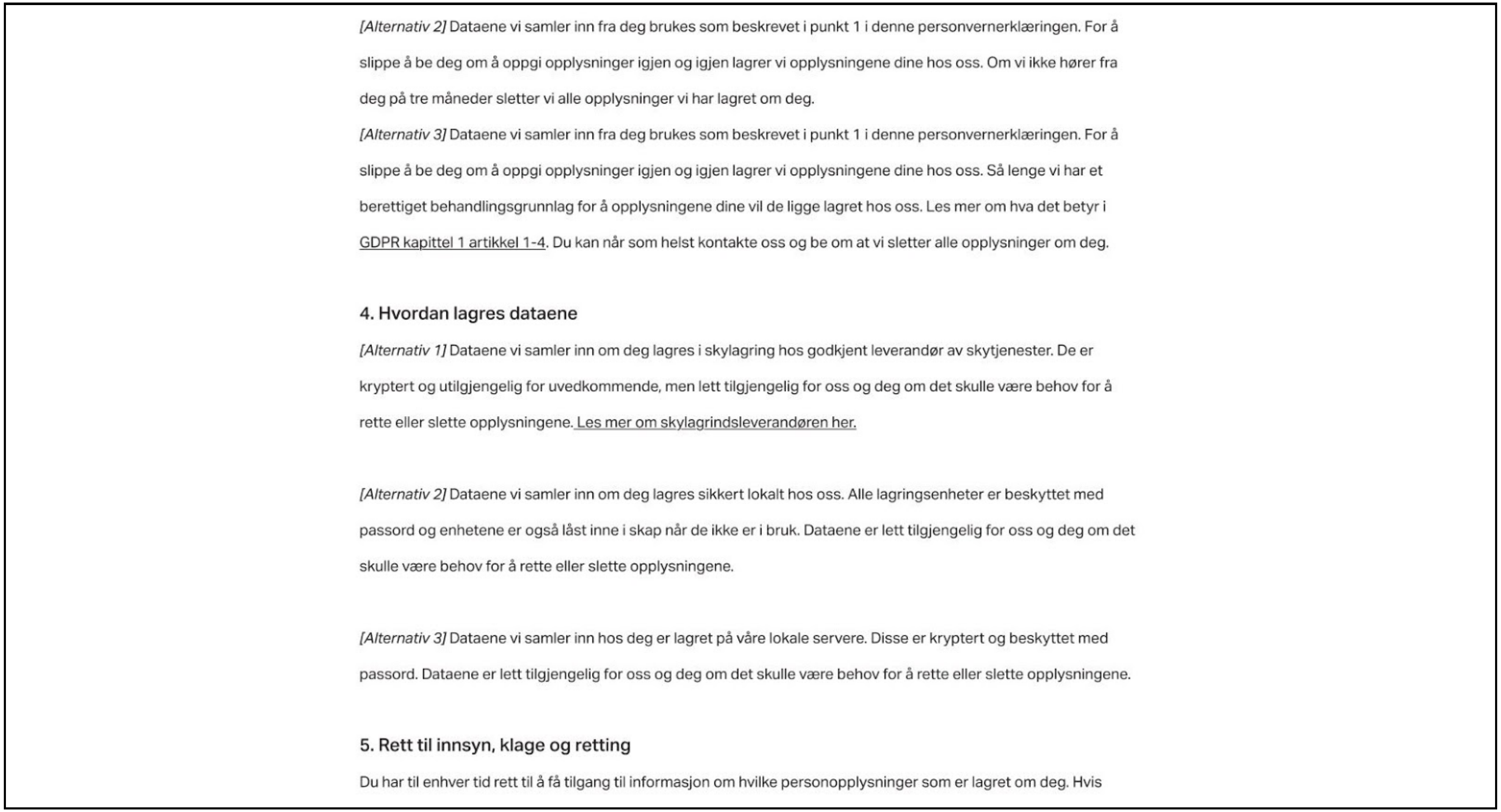
[Alternativ 2] Vi er en liten bedrift som ikke trenger alt for mye informasjon fra kundene våre, men noe er i fortsatt nødt til å vite. Noe behandling av personopplysninger skjer hos en samarbeidspartner, de forholder seg til samtykket du har gitt til oss og opererer under samme lover som Norge. Vil du vite mer kan du lese GDPR kapittel 4 artikkel 28-29.

[Alternativ 3] Vi er en liten bedrift som ikke trenger alt for mye informasjon fra kundene våre, men noe er i fortsatt nødt til å vite. Noe behandling av personopplysninger skjer hos en samarbeidspartner i utlandet. Vi har en egen databehandleravtale med bedriften som gjør at de må forholde seg til samtykket du har gitt oss og må behandle dataene iht GDPR. Vil du vite mer kan du lese GDPR kapittel 4 artikkel 28-29.

3. Hvor lenge skal dataene behandles

[Alternativ 1] Dataene du deler vil kun bli brukt til det formålet de samles inn og, så vil de slettes. Det vil si at når vi har utført vår tjeneste sletter vi umiddelbart opplysningene om deg. Skulle det bli behov for dem igjen en annen gang vil vi be deg om å oppgi dem på nytt.

10.8.11 Final result page pt 3 - Untailored



[Alternativ 2] Dataene vi samler inn fra deg brukes som beskrevet i punkt 1 i denne personvernerklæringen. For å slippe å be deg om å oppgi opplysninger igjen og igjen lagrer vi opplysningene dine hos oss. Om vi ikke hører fra deg på tre måneder sletter vi alle opplysninger vi har lagret om deg.

[Alternativ 3] Dataene vi samler inn fra deg brukes som beskrevet i punkt 1 i denne personvernerklæringen. For å slippe å be deg om å oppgi opplysninger igjen og igjen lagrer vi opplysningene dine hos oss. Så lenge vi har et berettiget behandlingsgrunnlag for å opplysningene dine vil de ligge lagret hos oss. Les mer om hva det betyr i GDPR kapittel 1 artikkel 1-4. Du kan når som helst kontakte oss og be om at vi sletter alle opplysninger om deg.

4. Hvordan lagres dataene

[Alternativ 1] Dataene vi samler inn om deg lagres i skylagring hos godkjent leverandør av skytjenester. De er kryptert og utilgjengelig for uvedkommende, men lett tilgjengelig for oss og deg om det skulle være behov for å rette eller slette opplysningene. Les mer om skylagrindsleverandøren her.

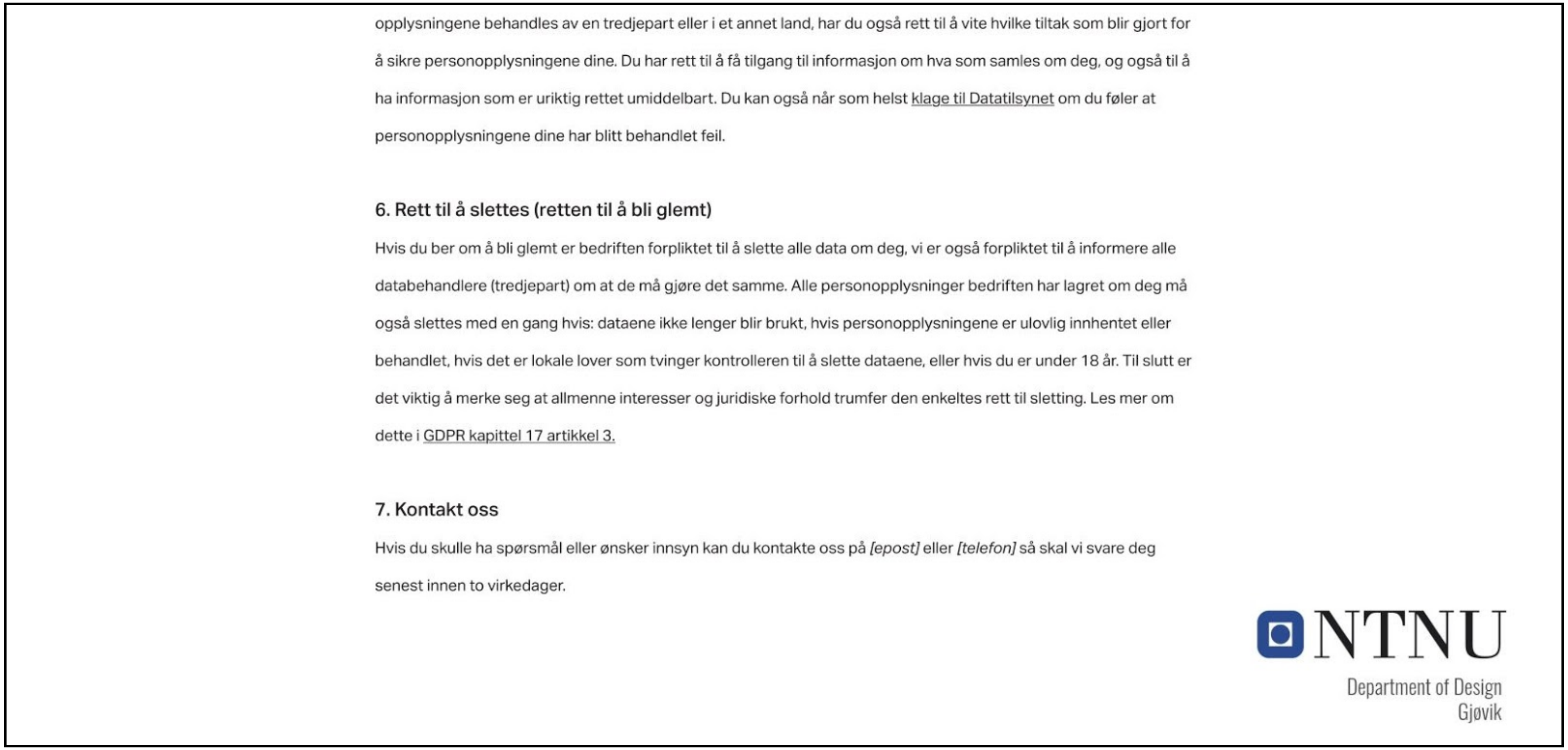
[Alternativ 2] Dataene vi samler inn om deg lagres sikkert lokalt hos oss. Alle lagringsenheter er beskyttet med passord og enhetene er også låst inne i skap når de ikke er i bruk. Dataene er lett tilgjengelig for oss og deg om det skulle være behov for å rette eller slette opplysningene.

[Alternativ 3] Dataene vi samler inn hos deg er lagret på våre lokale servere. Disse er kryptert og beskyttet med passord. Dataene er lett tilgjengelig for oss og deg om det skulle være behov for å rette eller slette opplysningene.

5. Rett til innsyn, klage og retting

Du har til enhver tid rett til å få tilgang til informasjon om hvilke personopplysninger som er lagret om deg. Hvis

10.8.12 Final result page pt 4 - Untailored



opplysningene behandles av en tredjepart eller i et annet land, har du også rett til å vite hvilke tiltak som blir gjort for å sikre personopplysningene dine. Du har rett til å få tilgang til informasjon om hva som samles om deg, og også til å ha informasjon som er uriktig rettet umiddelbart. Du kan også når som helst klage til Datatilsynet om du føler at personopplysningene dine har blitt behandlet feil.

6. Rett til å slettes (retten til å bli glemt)

Hvis du ber om å bli glemt er bedriften forpliktet til å slette alle data om deg, vi er også forpliktet til å informere alle databehandlere (tredjepart) om at de må gjøre det samme. Alle personopplysninger bedriften har lagret om deg må også slettes med en gang hvis: dataene ikke lenger blir brukt, hvis personopplysningene er ulovlig innhentet eller behandlet, hvis det er lokale lover som tvinger kontrolleren til å slette dataene, eller hvis du er under 18 år. Til slutt er det viktig å merke seg at allmenne interesser og juridiske forhold trumfer den enkeltes rett til sletting. Les mer om dette i GDPR kapittel 17 artikkel 3.

7. Kontakt oss

Hvis du skulle ha spørsmål eller ønsker innsyn kan du kontakte oss på *[epost]* eller *[telefon]* så skal vi svare deg senest innen to virkedager.

APPENDIX 9 - THE PRIVACY POLICY COPY (untailored)

Personvernerklæring for [FIRMANAVN]

1.Hvilke data vi samler inn og hvorfor

Vi vil gjerne *[kontakte deg / vise deg produkter akkurat du kunne vært interessert i / tilby deg skreddersydde løsninger / forbedre tjenestene våre / fyll inn selv for annet]* og derfor samler vi inn *[epost / telefonnummer / lokasjon / bilde /]*. Dette kan du når som helst velge å ikke dele og det vil ikke ha noen konsekvens for tjenestene vi tilbyr. Vi er derimot avhengig av *[navn /adresse / betalingsinformasjon]* for å kunne utføre tjenestene våre, dette utgjør et såkalt rettslig behandlingsgrunnlag. Du kan lese mer om det i GDPR kapittel 1 artikkel 1-4. Hvis du likevel ikke ønsker å dele denne informasjonen elektronisk kan du ta kontakt med oss direkte på telefon *[telefonnummer]* så finner vi en annen løsning der vi ikke lagrer noen av dataene dine.

2. Hvem skal behandle dataene

[Alternativ 1] Vi er en liten bedrift som ikke trenger mye informasjon fra deg, men litt er vi likevel nødt til å vite om kundene våre. Det er kun vi som behandler disse dataene, og det gjøres i henhold til GDPR som beskrevet i denne Personvernerklæringen.

[Alternativ 2] Vi er en liten bedrift som ikke trenger alt for mye informasjon fra kundene våre, men noe er i fortsatt nødt til å vite. Noe behandling av personopplysninger skjer hos en samarbeidspartner, de forholder seg til samtykket du har gitt til oss og opererer under samme lover som Norge. Vil du vite mer kan du lese GDPR kapittel 4 artikkel 28-29.

[Alternativ 3] Vi er en liten bedrift som ikke trenger alt for mye informasjon fra kundene våre, men noe er i fortsatt nødt til å vite. Noe behandling av personopplysninger skjer hos en samarbeidspartner i utlandet. Vi har en egen databehandleravtale med bedriften som gjør at de må forholde seg til samtykket du har gitt oss og må behandle dataene iht GDPR. Vil du vite mer kan du lese GDPR kapittel 4 artikkel 28-29.

3. Hvor lenge skal dataene behandles

[Alternativ 1] Dataene du deler vil kun bli brukt til det formålet de samles inn og, så vil de slettes. Det vil si at når vi har utført vår tjeneste sletter vi umiddelbart opplysningene om deg. Skulle det bli behov for dem igjen en annen gang vil vi be deg om å oppgi dem på nytt.

[Alternativ 2] Dataene vi samler inn fra deg brukes som beskrevet i punkt 1 i denne personvernerklæringen. For å slippe å be deg om å oppgi opplysninger igjen og igjen lagrer vi opplysningene dine hos oss. Om vi ikke hører fra deg på tre måneder sletter vi alle opplysninger vi har lagret om deg.

[Alternativ 3] Dataene vi samler inn fra deg brukes som beskrevet i punkt 1 i denne personvernerklæringen. For å slippe å be deg om å oppgi opplysninger igjen og igjen lagrer vi opplysningene dine hos oss. Så lenge vi har et berettiget behandlingsgrunnlag for å opplysningene dine vil de ligge lagret hos oss. Les mer om hva det betyr i GDPR kapittel 1 artikkel 1-4. Du kan når som helst kontakte oss og be om at vi sletter alle opplysninger om deg.

4.Hvordan lagres dataene

[Alternativ 1] Dataene vi samler inn om deg lagres i skylagring hos godkjent leverandør av skytjenester. De er kryptert og utilgjengelig for uvedkommende, men lett tilgjengelig for oss og deg om det skulle være behov for å rette eller slette opplysningene. Les mer om skylagrindsleverandøren her.

[Alternativ 2] Dataene vi samler inn om deg lagres sikkert lokalt hos oss. Alle lagringsenheter er beskyttet med passord og enhetene er også låst inne i skap når de ikke er i bruk. Dataene er lett tilgjengelig for oss og deg om det skulle være behov for å rette eller slette opplysningene.

[Alternativ 3] Dataene vi samler inn hos deg er lagret på våre lokale servere. Disse er kryptert og beskyttet med passord. Dataene er lett tilgjengelig for oss og deg om det skulle være behov for å rette eller slette opplysningene.

5. Rett til innsyn, klage og retting

Du har til enhver tid rett til å få tilgang til informasjon om hvilke personopplysninger som er lagret om deg. Hvis opplysningene behandles av en tredjepart eller i et annet land, har du også rett til å vite hvilke tiltak som blir gjort for å sikre personopplysningene dine. Du har rett til å få tilgang til informasjon om hva som samles om deg, og også til å ha informasjon som er uriktig rettet umiddelbart. Du kan også når som helst klage til Datatilsynet om du føler at personopplysningene dine har blitt behandlet feil.

6. Rett til å slettes (retten til å bli glemt)

Hvis du ber om å bli glemt er bedriften forpliktet til å slette alle data om deg, vi er også forpliktet til å informere alle databehandlere (tredjepart) om at de må gjøre det samme. Alle personopplysninger bedriften har lagret om deg må også slettes med en gang hvis: dataene ikke lenger blir brukt, hvis personopplysningene er ulovlig innhentet eller behandlet, hvis det er lokale lover som tvinger kontrolleren til å slette dataene, eller hvis du er under 18 år. Til slutt er det viktig å merke seg at allmenne interesser og juridiske forhold trumfer den enkeltes rett til sletting. Les mer om dette i GDPR kapittel 17 artikkel 3.

7. Kontakt oss

Hvis du skulle ha spørsmål eller ønsker innsyn kan du kontakte oss på [epost] eller [telefon] så skal vi svare deg senest innen to virkedager.

NTNU

Kunnskap for en bedre verden