Risk assessment: should the Norwegian Data Protection Authority create a Page on Facebook?

Final report 2021

Datatilsynet

Contents

Foreword

This report is based on an internal risk assessment of whether or not the Norwegian Data Protection Authority should establish a Facebook Page. The document's original and primary purpose was to enable the Authority's management to make a responsible decision on whether or not the organization should establish a Facebook Page.

We believe the assessment also would be of interest for the general public. The report summarizes our analyses, assessments and conclusions concerning risks, risk management and responsibilities pursuant to data protection legislation if the Norwegian Data Protection Authority, as a public authority, were to establish and communicate through a Page on Facebook.

In this assessment, the capacity of the Data Protection Authority is neither that of a supervisory authority nor that of an ombudsman, but rather that of a data controller, with the obligations that follow from this role under the General Data Protection Regulation (GDPR). This report, therefore, does not include general statements concerning the legality or liability of having a Facebook Page.

The original report was presented to the Data Protection Authority's management in March 2020. This public report has been supplemented with some clarifications, taking into account key developments in the field of privacy.

Summary

The Data Protection Authority aims to increase awareness of and interest in privacy in Norway. In order to achieve this goal, we are considering establishing a presence on various communication platforms for effective communication with important target audiences. We consider Facebook to be well suited for several of the Authority's communication needs and ambitions.

The implementation of the General Data Protection Regulation (GDPR) in 2018 introduced new rights for citizens and new obligations for organizations. As a result of this new Regulation, both private companies and public authorities have had to review their procedures, practices and purchases involving the processing of personal data to ensure compliance with the new Regulation. The obligations imposed by the Regulation also apply when an organization uses social media, e.g. a Page on Facebook.

In making sure the privacy of data subjects registered in a solution is protected, a Data Protection Impact Assessment (DPIA) is an important tool. The report presents a systematic description of the solution, including a legal assessment of accountability, an assessment of the necessity and proportionality of the processing, and considerations of measures to reduce privacy risks for the data subjects registered in the solution. The report also addresses considerations of a more ethical nature in light of the Data Protection Authority's values[1] and the Authority's position as a role model in privacy issues.

Conclusion

The Data Protection Authority's management team ultimately decided *not* to create and communicate through a Page on Facebook. The conclusion is based on an overall assessment, but has in particular emphasized the points below:

- The Working Party believes the risks to the data subjects' rights and freedoms associated with the Authority's processing of personal data through a Page on Facebook are too high.
- The Working Party believes that the Authority would not be able to implement measures to satisfactorily mitigate these risks.
- The Working Party's assessment is that the Data Protection Authority would not be in compliance with Article 26 of the GDPR on joint controllers.
- The Working Party finds it is not sufficient for the Authority to sign Facebook's standard arrangement on joint controllership. The Data Protection Authority will not be able to establish a separate arrangement with Facebook.
- The Working Party's assessment is that it would likely not be possible for the Data Protection Authority to fulfil the requirements of Article 25 of the GDPR on data protection by design and by default if we were to start using Facebook.
- The Authority's data protection officer recommends that the Data Protection Authority does not implement Facebook as a communication platform.
- The Working Party finds that the Data Protection Authority should place considerable emphasis on its position as a role model in matters related to data protection, as well as compliance with relevant privacy laws.

The analyses, assessments and recommendations of the Working Party have been documented in this report.

The report is based on an internal risk assessment of whether or not the Norwegian Data Protection Authority should establish a Facebook Page. In this assessment, the capacity of the Data Protection Authority is neither that of a supervisory authority nor that of an ombudsman, but rather that of a data controller, with the obligations that follow from this role under the GDPR (see preface).

[1] https://www.datatilsynet.no/om-datatilsynet/planer/datatilsynets-strategi/

Introduction

Our work began with an acknowledgement: Large parts of the public discourse have gone digital and are increasingly taking place on platforms owned by large, private technology corporations. Direct access to target audiences, being able to communicate with people where they are and where they spend their time, and being able to communicate with them in a way they like and are used to, make these platforms attractive to many organizations.

Participation in these platforms is user-friendly and seemingly free. From a privacy perspective, however, the situation looks a little different. Information about what we do on these platforms is collected on a large scale — to better understand us and our habits, and to provide us with tailored advertising and content. If a person creates a profile, or an organization creates a page on one of these platforms, it would normally entail a relatively extensive processing of personal data.

A data protection authority creating a page on such a platform may therefore seem somewhat contradictory. Nevertheless, the communication department believes the Authority should consider new channels of communication and new types of content suited for such channels, to participate and play a greater role in the public discourse. The idea is that these channels may contribute to effectively disseminate and host these types of content, generate increased traffic to the website and open up new arenas for debate and guidance. These considerations are among the reasons why we are considering Facebook as a communication platform.

The Data Protection Authority has a considerable interest in increasing visibility for our activities and areas of interest outside of our own domain (www.datatilsynet.no), and in increasing traffic to our website. Currently, we are producing a lot of new content, including a lot of audiovisual content, and we have employees with channel expertise and social media experience. We have also invested in equipment and competence for new types of content production. Furthermore, we believe that more channel-specific communication, such as comment sections, networking and relation-building, could extend the reach of our role as ombudsman.

At the same time, we must be aware that having a presence on Facebook comes with additional commitments. This includes dedicating sufficient resources, efforts to engage target audiences with good and relevant content tailored to the unique characteristics of the channel, and regularly evaluating the channel's effectiveness, usefulness and terms and conditions.

Objectives

On this basis, we formulated two objectives for creating and communicating through a Page on Facebook.

- *Objective 1:* Informing and engaging Norwegian Facebook users about privacy laws, privacy considerations and other, related topics, and informing users about the Data Protection Authority's core activities.
- *Objective 2:* Promoting discussion of privacy laws and privacy considerations, and inviting Norwegian users in to discuss and develop the topic of privacy and the Data Protection Authority's role in social development.

One side effect of using a Page on Facebook would be that the Data Protection Authority would gain insight into communication on the Page, such as statistics on demographics and interactions. Aggregated insight data is default for owners of a Page on Facebook and cannot be turned off. We did, however, choose not to formulate this as a separate objective.

We do not wish to use the platform's advertising service or integrate Facebook widgets, plug-ins or other features on our own website. Analyses and assessments of these features will therefore not be discussed in this report.

Risk assessment

The assessment should provide the organization's Management Team with a basis for an informed and sound decision on whether the Data Protection Authority, as a data controller, should create and communicate through a Page on Facebook.

Organization and background work

The use of Facebook as a communication platform has been discussed internally within the Data Protection Authority before; however, no true assessment of such use of the platform from the perspective of compliance with relevant privacy laws has been performed.

To conduct the assessment, we appointed an interdisciplinary group comprised of experts in law, technology and media.

The mapping and analysis are primarily based on Facebook's privacy policy[2] and other publicly available material provided by Facebook. This analysis material was primarily collected in the period from July 2019 through February 2020. In addition, we have collected documentation from other sources we have deemed suitable for shedding light on data processing and the risks inherent in use of the platform. Judgments, decisions, guides and other legal usage have been applied to clarify and assess the Authority's joint controllership with Facebook.

Parties and roles

This assessment seeks to clarify roles and responsibilities. In using Facebook, several types of parties would be involved: the provider (Facebook), the Page owner (Data Protection Authority), users (data subjects) and other parties (e.g. advertisers, subproviders and Facebook's partners). In this assessment, we believe it is especially important to identify and, to the greatest extend possible, clarify the roles and responsibilities of the Data Protection Authority and Facebook, respectively, in terms of processing.

Roles and responsibilities in social media have been considered in rulings by the European Court of Justice, specifically Wirtschaftakademie (C-210/16)[3] and Fashion ID (C-40/17)[4]. Both these cases establish that interaction between social media and other parties may constitute joint controllership pursuant to Article 26 of the GDPR. Whenever joint controllership is present, this report seeks to clarify how responsibilities potentially could be distributed between Facebook and the Data Protection Authority. The rulings were issued pursuant to previous legislation, but the transfer value to the new legislation is high, and possibly also more stringent.[5]

Execution

In this assessment, we have applied the Data Protection Authority's own templates for risk assessments and DPIAs. These templates serve as a general framework for designing and performing the analysis and assessments.

Chapter IV of the Regulation stipulates constraints and requirements to which the data controller is subject. We have structured the analysis, assessments and this report based on a procedure developed by the Data Protection Authority itself.[6] The process is illustrated below, at the end of this section. It addresses the obligations with which the data controller must comply at all times, as well as obligations that apply if the processing is presumed to be associated with high risk to the data subject's rights and freedoms.

We begin by preparing a *systematic description of the data processing* associated with having a Page on Facebook. The objective is for us, as the data controller, to gain a comprehensive overview of the processing and to ensure that the descriptions are complete and clear. The descriptions are seen in light of Articles 24, 30, and

---

[2] https://www.facebook.com/policy.php

[3] C-210/16 *Wirtschaftsakademie* Press release: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081en.pdf

[4] C-40/17 *Fashion ID*. Press release: https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf

[5] See, for example: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/ny-dom-fra-eu-domstolen-om-fellex|s-behandlingsansvar/

[6] https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf

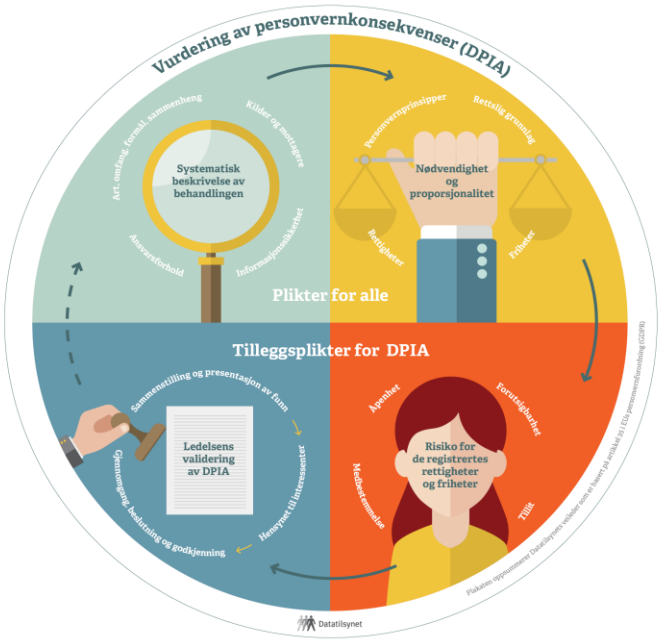
32 of the GDPR. This description covers the nature, scope, purpose and context of processing, sources, recipients and accountability, as well as information security, including identification of information security risks. In addition, we also assess our compliance with the provisions concerning joint controllership with Facebook pursuant to Article 26 of the GDPR.

We then assess the necessity and proportionality of the data processing. The objective is to ensure that the choices we make in our capacity as data controller are legitimate and performed in such a way that the processing is proportionate to the purpose(s). We assess whether data protection principles (Articles 5, 6 and 9), the rights of data subjects (Article 12-22), and the freedoms of the data subjects (Preamble 4 and Article 8 of the ECHR) are protected. We also briefly account for our assessment of whether our use of a Page on Facebook is in compliance with the rules on data protection by design and by default under Article 25.

Based on the mapping of the nature, scope, purpose and context in the systematic description, we concluded that the risks to the data subject's rights and freedoms were high. In our assessment of necessity and proportionality, we found that it would be difficult to implement measures that would satisfactorily mitigate these risks. That is why we also conducted a data protection impact assessment (DPIA, Article 35) to see whether it would still be possible for us to do the processing. A DPIA requires a flipping of perspectives — from focusing on the Authority's own duties, to considering the processing from the perspective of the data subject.

The Working Party has consulted with the Data Protection Authority's data protection officer (DPO) in accordance with Article 35 (2). The DPO's views have been included in this report.

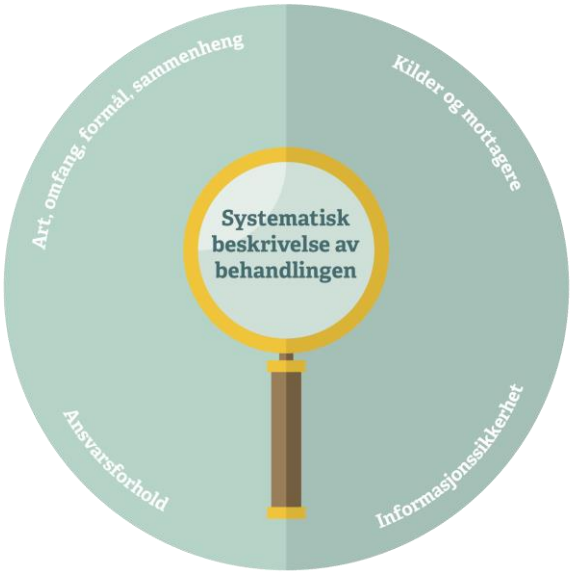
This work leads to a conclusion and a recommendation to the management team.



"DPIA Data Wheel" (Norwegian): This figure summarizes and illustrates the general process of conducting a data protection impact assessment (DPIA).

Systematic description of the data processing

Below, we provide a systematic description of the data processing by considering its nature, scope, purpose, context, sources, recipients, responsibilities and data security, cf. the figure below. The goal is to establish a detailed overview of the processing and to identify risks associated with the use of a Page on Facebook. We always strive to separate the Data Protection Authority's processing activities from those of Facebook.



Nature, scope, purpose and context

Nature of processing
The description of the nature of processing focuses on the inherent characteristics of processing:

Collection: Personal data will be collected from content created by the data subject[7], i.e. posts and engagement, either in relation to the Authority's own posts, or in two-way communication with users. In addition, Facebook will collect observation data[8] and derive new data on users[9] who interact with the Authority's Page.

Storage: The Data Protection Authority is entirely at the mercy of how Facebook chooses to store and cache the personal data, as well as how Facebook chooses to share personal data with sibling companies and other partners. Personal data is shared globally.[10][11]

Use: The Data Protection Authority will use personal data to provide information, generate discussion and collect aggregated statistics. Among other things, Facebook can compile personal data generated through the Authority's Page across its products to provide and support its products and services, as well as to provide customized content to users. Facebook will also analyze personal data for profiling and to provide personalized information and ads.[12]

Access to data: The public will have access to all information shared on the Page. The Authority's editor/moderator will have access to direct messages and drafts. In theory, Facebook will have access to all communication on the Page, and could also give access to a range of third parties.[13]

About whom is data collected? The Data Protection Authority will collect personal data from employees, article authors and other partners, as well as any person or entity who chooses to interact with the Authority's Page.

How can data subjects exercise their rights? The Data Protection Authority will be able to assist the data subject to some degree, but this is limited to providing information about the processing itself and to guiding users in how to exercise their rights on the platform. The Authority's moderator will be able to correct and delete information on our Page in response to a direct request, but this information will still be available to Facebook. Users will be able to exercise many rights under the

---

[7] https://www.facebook.com/policy.php ("What kinds of information do we collect?")

[8] Also includes data points for use in Page Insights for Page owners: https://www.facebook.com/legal/terms/page_controller_addendum

[9] https://www.facebook.com/about/privacy/update ("How do we use this information?")

[10] Ibid. ("How do we operate and transfer data as part of our global services?")

[11] https://www.facebook.com/legal/terms/ ("The services we provide")

[12] https://www.facebook.com/about/privacy/update ("How do we use this information?")

[13] Ibid.

GDPR on dedicated pages on the platform or in the user interface.[14][15][16]

Will there be systematic processing of personal data? The Data Protection Authority's use of the Page will be targeted and strategic, in line with certain editorial goals and the Authority's communication plan, but the Authority will not engage in systematic processing of personal data. Facebook continuously performs systematic processing of all personal data generated on the Data Protection Authority's Page.[17]

Use of new technology/new use of existing technology: For the Data Protection Authority, creating and using a Page on Facebook would be considered implementation of a new technology. As far as we know, we are the first organization in Norway to conduct a major analysis and assessment of whether using a Page on Facebook would be compliant with the GDPR. Facebook uses evolving and innovative technology, which entails new types of processing.[18] A technology that is innovative and evolving by nature, and that has dynamic terms and conditions,[19] could have practical and unpredictable implications for our internal control and our assessments in the systematic description of Facebook, our legal responsibility as the (joint) controller, and for the communication itself on the platform.

Scope of processing
The description of the scope of processing includes:

Categories of personal data: Of the content the Data Protection Authority itself wishes to share on the Facebook Page, we believe this will primarily be general personal data, not subject to Article 9 of the GDPR on the processing special categories of personal data. However, we need to make reservations concerning personal data revealed through visual and audiovisual content. We also have some experience from our guidance service, and we know that many vulnerable people contact the Data Protection Authority, wanting to share very private and detailed personal data, which would be subject to Article 9. We cannot rule out that the same type of inquiries would occur if the Data Protection Authority is present on Facebook, and users may share a wide range of types of personal data. Furthermore, Facebook will collect information and content provided by users, information about pages users interact with, as well as device information/meta data and observation data.[20] From this data, Facebook could derive new categories of personal data and build profiles of people.[21]

Number of data subjects: It is hard to estimate the number of data subjects. We can, however, estimate that the Data Protection Authority's maximum reach in terms of users will be approx. 100,000 users over a five-year period. There are approx. 3.5 million Norwegian Facebook users. Worldwide, there are approx. 2.5 billion Facebook users.[22]

Volume of data: All personal data, voluntarily provided, in combination with observation data and meta data, can be multiplied by approx. 100,000 users.[23] As such, the number of variables and the level of detail will be complex and unclear to us. For Facebook, this profiling, reconciliation and derived data on these 100,000 users come in addition to all other behaviours and use of the platform. Facebook also collects personal data from outside the platform and through other partners,[24] and could potentially reconcile this data with personal data generated through the Data Protection Authority's Page. Facebook is one of the companies in the world that processes the most data.

Frequency: The Data Protection Authority's moderator would monitor and moderate the Page daily and regularly, but in practice, the Authority would process personal data for its own purposes on a continuous basis. Facebook continuously, systematically and

---

[14] Ibid.

[15] See also: https://www.facebook.com/settings

[16] See also: https://www.facebook.com/help/contact/367438723733209

[17] https://www.facebook.com/about/privacy/update ("What kinds of information do we collect?")

[18] Ibid. Such as product development, research and innovation ("How do we use this information?")

[19] https://www.facebook.com/legal/terms/update ("Additional provisions")

[20] https://www.facebook.com/about/privacy/update ("What kinds of information do we collect?")

[21] Ibid. ("How do we use this information?")

[22] E.g. Statista: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[23] Hypothetically.

[24] https://www.facebook.com/about/privacy/update ("What kinds of information do we collect?")

automatically processes personal data,[25] including personal data from the Data Protection Authority's Facebook Page.

Storage period: The Data Protection Authority would assess the relevance and currency of information on the Page at least once a year. Outdated information would be deleted. We believe that the maximum storage period for information on our Page would be five years. How long personal data remains Facebook's system is determined by Facebook on a case-by-case basis, and would depend on the nature of the data, why it was collected and processed, and relevant legal or operational storage requirements. Facebook also states that they delete information in the sense that the data is made unavailable to users. At the same time, Facebook claims to delete data when it is no longer necessary.[26]

Geographical scope: The Data Protection Authority's content is intended for a Norwegian audience, and we have the option of limiting the Page and the visibility and accessibility of posts based on country. Facebook collects, stores and distributes personal data in its own infrastructure, with data centres and systems all over the world.[27] The company also uses standard contractual clauses approved by the European Commission as a basis for transfer.[28][29] Our assessment was made before the European Court of Justice's ruling in the Schrems II case (C-311/18)[30] was issued, and we have therefore not looked into any additional measures implemented by Facebook as a result of this ruling. Personal data generated through the Data Protection Authority's Page on Facebook would be subject to the same structure, and we must expect that the data will be stored and processed from anywhere in the world.

Purpose of processing

The description of the purpose of processing seeks to emphasize what the personal data will be used for:

Purpose: The Data Protection Authority's purpose of processing is public education and debate. To the extent Facebook has an overall purpose, the following statement can be found on Facebook's front page: "Give people the power to build community and bring the world closer together." However, Facebook processes personal data for a wide range of purposes: 1) Provide personalized services and improve on these; 2) provide measurements and analytics in support of its partners, such as advertisers; 3) promote safety to detect unwanted material and to protect the integrity of its products; 4) communicate with users and assist them; and 5) support research and innovation.[31]

Control purposes[32]: The Data Protection Authority does not use personal data for control purposes. Our assessment is that Facebook likely does not use personal data for control purposes.

Are decisions about the data subject made on the basis of systematic and comprehensive analyses of personal data? The Data Protection Authority does not use personal data to make decisions about the data subject on the basis of systematic and comprehensive analyses. We believe Facebook uses personal data to make decisions about the data subject on the basis of systematic and comprehensive analyses.[33]

Decisions that significantly affect the data subject: The Data Protection Authority does not use the personal data to make decisions that significantly affect the data subject. Our assessment is that the decisions Facebook makes about the data subject do *significantly* affect the data subject, in that Facebook decides who sees what, which in turn could affect the data subject's choices and decisions. It is debatable, however, whether the decisions Facebook makes about the data subject are subject to Article 22 of the GDPR. In any event, our assessment is that data generated through our Page does not, to any significant degree, contribute to the overall basis for decision-making.

---

[25] Ibid.

[26] Ibid. ("Data retention, account deactivation and deletion")

[27] Ibid. ("How do we operate and transfer data as part of our global services?")

[28] https://www.facebook.com/help/566994660333381?

[29] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[30] C-311/18 *Schrems II*. Press release: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[31] https://www.facebook.com/about/privacy/update ("How do we use this information?")

[32] Cf. section 3 "Purpose of processing" in the guide: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10362

[33] Additional examples are listed under "How do we use this information?" https://www.facebook.com/about/privacy/update

Profiling: The Data Protection Authority does not use personal data for profiling purposes. We believe it is reasonable to assume that Facebook uses personal data to build profiles on its users, including data generated though our Page.

Reveal hidden traits/recognize patterns: The Data Protection Authority does not use personal data to reveal hidden traits or recognize patterns in the user. We believe it is reasonable to assume that Facebook also will use personal data generated through our Page to reveal hidden traits or recognize patterns in the user.

Reprocessing of personal data for new purposes: The Data Protection Authority does not use personal data collected through our Facebook Page to reprocess the data for new purposes. In our assessment, Facebook's wide and vague purposes[34] means it is difficult to say what is processed for the original purpose and what is processed for so-called *new* purposes.

Context of processing

The description of the context of processing focuses on the context in which the data is processed:

Sources: The Data Protection Authority will collect personal data directly from the user's posts and the built-in interaction options in the platform. We could also choose to curate or share content from other parties on or outside Facebook. Aggregated statistics on interaction on our Page comes from Facebook. Facebook will have access to all information generated through the Authority's Page on the platform. Beyond the platform and the domain, Facebook generates personal data from, among other things, website integrations and plugins (such as the "like" button) cookies[35], subsidiaries, partners, advertising agencies and the users' devices.[36]

Relation: The Data Protection Authority is both an ombudsman and a supervisory authority. In other words, we are a public authority, and users may perceive us as an authority with the power to make decisions and as a body that potentially has considerable leverage and expertise. For many users, we may be perceived as a trusted party and as a "saviour" and/or guarantor in issues related to privacy and data protection. It is debatable whether users would perceive interactions with us on Facebook as communication with an authority or as communication with any other Facebook Page. As communication with public and private parties on Facebook has become more normalized, there is reason to expect that the data subject would act differently with a supervisory authority on Facebook than they would with the same supervisory authority through other channels and in other contexts. Knowledge about people is power, and Facebook would be in possession of a lot of and significant personal data about users. Our assessment is that Facebook would also be in possession of data the user most likely is not aware of.

The data subject's control over their own personal data: The user can delete and edit their own posts and engagement with the Data Protection Authority's Page. The Data Protection Authority can also assist in deleting information from the Page. Posts already shared by other users cannot be deleted by the user, and can also not be deleted by the Data Protection Authority (unless the posts have been shared on our Page). Facebook can delete information, but in our experience, it is difficult to establish contact with Facebook as the owner of a Page or as a user. We believe it can be difficult for the user to maintain an overview of their own interaction with the Data Protection Authority's Page *over time*. We also believe it can be difficult to stay in control of and maintain an overview of the use, scope and consequences of Facebook's reprocessing of personal data generated through the Page.

Predictability of processing for the user: We will strive to ensure that the Data Protection Authority's processing for our purposes — our communication activities — will be interpreted as limited in scope, clear, predictable and professional. Most Facebook users will be used to communicating with Pages, and as such, this processing may be perceived as predictable. Nevertheless, there are likely several aspects of the processing that may be perceived as unpredictable. Many will not have a clear understanding of the scope, visibility and public nature of their posts and interactions on the platform, including their interaction with Pages. The user may not understand the *viral* power of information, which in this context refers to its potential of being spread outside of our Page through sharing, tagging and news feeds. The data subject may provide too much personal data, including special categories of personal data, in what may be

---

[34] Ibid. (("How do we use this information?")

[35] About cookies: https://www.facebook.com/policies/cookies/

[36] https://www.facebook.com/about/privacy/update

misperceived as a kind of confidential dialogue with the Data Protection Authority, either publicly or through direct messages. The individual user may misinterpret the Data Protection Authority's presence as a guarantee that the platform is more data protection-friendly than it really is. Many may not be aware that all interactions a user has with the Data Protection Authority's Page will be collected and compiled with other data Facebook has collected about them. Many will not know that the data generated about them through the Data Protection Authority's Page could be stored globally and may be shared with a wide range of sibling companies, partners and third parties. Many will likely also not be aware of the scope of data generated about them over time, or of the "memory" Facebook has about them.

Special expectations of confidentiality: We believe most users do not have a *special* expectation of confidentiality. Even so, it would be reasonable to expect that many do not know what they can or should expect in terms of confidentiality, such as children or users with limited experience or competence. Some likely expect confidentiality in the Page's direct messaging function.[37] Finally, it is our assessment that data will be processed in a number of ways of which the user is not aware and therefore also cannot expect.

Special expectation of necessary and accurate data: Users largely provide their own personal data, including statements and engagement. Facebook will derive new information about the user, generated from the Data Protection Authority's Page. The data subject will have limited knowledge of whether this derived data, or profiling, is accurate — or of how important "accuracy" is for the decisions Facebook makes about users.

Special expectations of privacy: Many users have a general idea of how Facebook operates, and will not have any such expectations. But it would be reasonable to assume that many do not know what they can or should expect in terms of privacy on social media, such as children or users with limited experience or competence. It would likely also surprise many how detailed, close and "intimate" Facebook can get to collect and process certain types of personal data, not least considering its combination of several types of data. Many users may misinterpret the direct messaging function as a truly private or more confidential channel (in line with closed groups on Facebook).

Personal data about children, patients or other vulnerable categories of individuals: The Data Protection Authority will not publish personal data about identifiable, vulnerable categories of individuals on our Page. At the same time, we have to take into consideration that vulnerable categories of individuals may choose to interact with the Page and provide information about themselves, ,and that other users may provide personal data about such individuals. Facebook will process data about vulnerable categories of individuals if such data is generated through the Page. Facebook has a minimum age of 13 years old for users. Even so, we know that Facebook is used by children younger than 13.[38]

Previous experience with similar types of processing: As far as we know, no one has conducted an analysis and risk assessment pursuant to the GDPR of a data controller who wants to create and use a Page on Facebook. There are similar types of communication platforms that *may* have similar types of processing, such as Instagram, Twitter, LinkedIn, etc.

*Potential relevant advancements in technology or security***:** The company regularly announces that they have implemented measures to promote data protection in its products.[39] On their blog, they write that the new design will focus on Facebook groups and events, as these, in Facebook's opinion, make the platform more private and data protection-friendly.[40] We are also aware that Facebook has defined a vision of introducing encryption for certain types of data, which means Facebook would not itself be able to access the data. Another suggestion from the company is to set time limits and duration, which would entail that certain types of data would be removed automatically as a default setting[41].

General concerns about how the processing of personal data is described: In recent years, Facebook has been under constant media scrutiny and pressure from authorities and organizations concerning the company's

---

[37] E.g.: https://www.an.no/nyheter/norsk-advokat-ble-overvaket-av-usa-pa-facebook/s/1-33-6704657

[38] See e.g.: https://medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/200211-barn-og-medier-2020-delrapport-1_-februar.pdf

[39] https://about.fb.com/news/tag/privacy-matters/

[40] https://www.dn.no/medier/mark-zuckerberg/messenger/whatsapp/mark-zuckerberg-endevender-facebook-designet/2-1-595876

[41] https://about.fb.com/news/2019/03/vision-for-social-networking/

compliance with data protection legislation and respect for individuals' privacy and data protection.[42] In January of 2020, one of the German supervisory authorities, *Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg* (LfDI) chose to close its Twitter account[43][44] due to the judgments related to Article 26 on joint controllership, based on a lack of compliance with the GDPR.

Processing of personal data from different data sets, for different purposes, from different data controllers, and linking to different registers to generate a new type of data about the data subject: The Data Protection Authority will not process personal data from different data sets or link different registers to generate new types of data about the data subjects. Facebook, as well as various subsidiaries and third parties, may potentially use data and data sets with personal data generated from the Data Protection Authority's Page. Our assessment is that personal data imported from other partners is linked to existing users.[45]

Responsibilities, sources and recipients

The description of sources and recipients gives an overview of recipients, data flow and storage:

Identification of data controller, joint controllers and data processors: In some areas, the Data Protection Authority and Facebook will be separate data controllers. However, the Data Protection Authority and Facebook will be joint controllers for some activities. Our assessment is that there would be joint controllership between Facebook and us as the Page owner. We have not been able to find a list of other data processors and subproviders that is available to the public. We have also found Facebook's contract with Page owners concerning joint controllership, "Facebook Page Insights".[46] This is non-negotiable and only covers some of the processing activities where we believe we would have joint controllership with Facebook. We account for joint controllership in Appendix 1 to this report.

Identification of the recipient of personal data: All information in and engagement with public posts on our Page on Facebook would, in practice, be available to anyone. In addition, the Authority's editor and moderator will have access to the Page's direct messages and aggregated statistics. Facebook transfers data within the Facebook group,[47] to service providers and third parties, as well as other parties.[48] Facebook transfers personal data to countries outside the EU/EEA.

Identification of data flow, storage and caching: Facebook transfers personal data globally, both internally within Facebook companies and externally to its partners and users[49]. We have not been able to find a flow chart outlining where and how long personal data is stored in various locations. See also "Storage" on page 10

Personal data security

In this description, we assess whether personal data security is sufficiently protected pursuant to Article 32.

Risks associated with personal data security are related to the links between value, threats/threat agents and vulnerabilities. Our specific assessment of these factors, as well as of measures intended to mitigate risks related to personal data security, is presented in Appendix 2 to this report.

Facebook describes its internal organization of data processing security[50][51]. If we were to start using Facebook, we must be aware that we have to accept the premise for security Facebook sets with Page owners at any given time. We believe, however, that Facebook wants and has implemented measures aimed at protecting its internal data security. Facebook claims[52] that they annually undergo a third-party SOC 2 type II

---

[42] Perhaps best exemplified by the Cambridge Analytica case: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

[43] https://www.baden-wuerttemberg.datenschutz.de/bye-bye-twitter/

[44] LfDI clarifies important requirements for authorities' use of social media in a press release: https://www.baden-wuerttemberg.datenschutz.de/lfdi-stellt-wesentliche-anforderungen-an-die-behoerdliche-nutzung-sozialer-netzwerke-klar/

[45] https://www.facebook.com/about/privacy/update (several sections)

[46] https://www.facebook.com/legal/terms/page_controller_addendum

[47] https://www.facebook.com/help/111814505650678

[48] https://www.facebook.com/about/privacyshield

[49] https://www.facebook.com/privacy/explanation

[50] https://www.facebook.com/legal/terms/dataprocessing

[51] https://www.facebook.com/legal/terms/page_controller_addendum

[52] https://www.facebook.com/legal/terms/dataprocessing

audit in relation to its data processing services, as well as other industry standard audits deemed appropriate by Facebook as part of Facebook's audit programmes. SOC 2 deals with internal audits related to data security in general. We are not sure which other industry standard audits Facebook deems appropriate in addition to this.

Summary and assessment: systematic description of the data processing

In this chapter we have presented a description of the data processing of personal data associated with creating and communicating through a Page on Facebook. By describing the nature, scope, purpose and context of data processing, we are able to risks to the data subject's privacy, rights and freedoms. We have summarized the risks and the Working Party's assessments of these risks below:

Risks associated with the nature of processing:

- The Working Party believes it is difficult for the Data Protection Authority to help the data subject exercise their rights pursuant to the GDPR vis-à-vis Facebook.
- The Working Party believes that the processing of personal data is characterized by unpredictability.
- The Working Party believes that the processing of personal data is characterized by a lack of transparency vis-à-vis the data subject.
- The Working Party believes that there are uncertainties associated with compliance with several data protection principles.
- The Working Party believes that our communication on a Page would entail systematic processing in the form of profiling and automated decision-making.
- The Working Party believes that questions concerning the potential of an unequal power balance between the company and the user may be problematic.
- The Working Party believes that this involves innovative technology that is constantly changing.

Risks associated with the scope of processing:

- The Working Party believes that the processing will include many different categories of personal data, including, potentially, special categories of data.
- The Working Party believes that the processing potentially could entail the processing of personal data about vulnerable individuals.
- The Working Party believes that the processing involves a large number of data subjects.
- The Working Party believes that the volume of personal data about the data subject is large and detailed.
- The Working Party believes there are some uncertainties concerning storage periods, including potentially permanent storage.
- The Working Party believes that the geographical scope of storage is global, which includes areas outside the EU/EEA.

Risks associated with the purpose of processing:

- The Working Party believes that Facebook's purposes are vague, unclear and comprehensive. We believe that they largely diverge from the purposes the Working Party has defined for processing.
- The Working Party is uncertain of whether personal data will be used for new or alternative purposes.
- The Working Party believes that the decisions made about the data subject may significantly affect the data subject.
- The Working Party believes that decisions made about the data subject are based on systematic and comprehensive analyses of personal data.

Risks associated with the context of processing:

- The Working Party believes there are several uncertainties associated with sources, data sets, and compilations of data sets within and outside of the platform.
- The Working Party believes the data subject could have an expectation of confidentiality and privacy in certain types of communication with a Page on the platform.
- The Working Party believes it is difficult for the data subject to stay informed and in control of their own data.
- We believe data flows and chains of processing are unclear, including who the recipients of personal data are.

In our assessment of joint controllership (Appendix 1), we have made an effort to map the roles and responsibilities of the Data Protection Authority and Facebook in data processing. The Working Party has concluded as follows:

- The Data Protection Authority has joint controllership with Facebook if the Authority creates a Page on Facebook, ref. the Fashion ID and Wirtschaftsakademie judgments.

In our assessment, the Data Protection Authority and

Facebook would, at the very least, be joint controllers of the following:

- The Data Protection Authority and Facebook would be joint controllers of the collection of personal data about users visiting or interacting with the Data Protection Authority's Facebook Page.
- The Data Protection Authority and Facebook would be joint controllers of outcome of the analysis of personal data about users visiting or interacting with the Data Protection Authority's Facebook Page ("Page Insights").
- The Working Party believes it is uncertain whether the Data Protection Authority will have some level of joint controllership for Facebook's use of personal data about users visiting the Data Protection Authority's Facebook Page to enrich user profiles for the purpose of providing personalized content and advertising.

As a consequence of acknowledging joint controllership, we also believe that:

- The Data Protection Authority and Facebook share a joint responsibility for informing users, in a transparent, accessible and understandable way, of what their personal data will be used for.
- Facebook and the Data Protection Authority have a joint responsibility for protecting the rights and freedoms of data subjects.

We find the Data Protection Authority's compliance with Article 26 of the GDPR to be as follows:

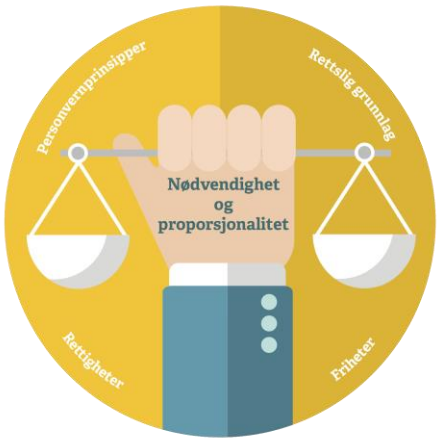
- The Data Protection Authority will *only partially* be compliant with Article 26 (1) of the GDPR.
- The Data Protection Authority will *only partially* be compliant with Article 26 (2) of the GDPR.
- The Data Protection Authority will *not* be compliant with Article 26 (3) of the GDPR.

Further, we have summarized our assessment of whether the processing protects data security (Appendix 2):

- In the value assessment, we concluded that our integrity requirement for the value *Public communication* (information the Data Protection Authority chooses to post on the platform, cf. Purpose 1) on the Page is "high". We also concluded that our requirements for confidentiality and integrity are "very high" and "high", respectively, for the value *Communication with users* (comments, direct messages, engagement and other interactions between the Data Protection Authority's Page and users, cf. Purpose 2).
- In the threat assessment, we have identified and described a selection of what we believe to be the most relevant threats/threat agents. This includes ordinary users, children, mentally unstable individuals, online activists, trolls and Data Protection Authority employees.
- In the vulnerability assessment, we have described our presumed vulnerabilities in relation to processing, including, e.g., posts without clarification, lack of control over comments and the information flow of the Page, or poor access control.
- We believe certain risks associated with personal data security in data processing can be mitigated by implementing certain measures, e.g. by establishing procedures and responsibilities for moderation, activating two-factor authentication, and defining roles and responsibilities.
- Our assessment is that we have to be able to trust that Facebook is capable and competent in protecting its internal information security.

Necessity and proportionality of processing — a balancing of interests

In this chapter, we assess and ensure that the processing, as systematically described in the previous chapter, is necessary and proportionate. This entails assessing the legal basis for the processing, the protection of privacy principles and the rights and freedoms of users, cf. the figure below (Norwegian).



Legal basis

The Data Protection Authority's legal basis for creating and using a Page on Facebook is derived from Article 6 (1) (f) of the GDPR on the balancing of interests. This legal basis provides us, as an organization, with the right to process personal data if it is necessary to pursue a legitimate interest, unless this interest is overridden by considerations of the data subject's privacy.

Facebook uses several different legal bases for processing vis-à-vis the individual user, depending on the type of processing involved, such as performance of a contract, consent, legitimate interests, public interest and legal obligation[53].

The Data Protection Authority's interests:
The Data Protection Authority's interests are legitimized in purpose 1 and purpose 2, which are defined in the introduction of this report.

How does the Authority benefit from processing, and how important are these benefits for the Authority?

Many of the benefits associated with creating and communicating through a Page on Facebook are described in the introductory chapter of this report. In many ways, our communication department considers being present through a Page on Facebook as a "luxury channel". By this we mean that this channel neither replaces nor innovates the Authority's communication activities as such. Communication through this channel would rather be a supplement to other communication. It could make us *more* accessible by target groups, *increase* visibility and knowledge of our message and of the Authority in the general public, and achieve *greater* impact of content we have already produced, and measures we have already implemented. In addition, the channel is well-suited for communicating multimedia content, and the Authority's video and live-streaming content could benefit from this. The channel could also make it easier to be a *more* active and distinct voice in the data protection discourse, while also *increasing* democratic participation.

Is the processing carried out in the public interest or does it protect ideal interests that would benefit others?

We believe that being present on Facebook would serve the main purpose of being in the public interest. We argue that our presence in this channel would make us more open and accessible, and that it would facilitate for greater involvement from Norwegian citizens. Our presence on the channel would give Facebook users, i.e. citizens, access to clear, correct and updated information about their personal data rights and obligations according to law, access to news and information about the Data Protection Authority's activities and interests, and an invitation to participate in the data protection discourse with the Data Protection Authority as the moderator. This interest is particularly justified, in that many use this channel as their primary source of information and news, where users personally subscribe to individuals, organizations or brands they are interested in. This means that we also, to a greater extent, are able to reach citizens with news and information they "did not know they needed" in their daily information feed, instead of only providing them with information when they actively search for it.

[53] See full overview: https://www.facebook.com/privacy/explanation

Considerations of privacy:
By creating a Page on Facebook, it would generate a wide range of personal data and enable several types of data processing, both for the Data Protection Authority and for Facebook. In the systematic description, we summarize many different assessments of risks and considerations of privacy. Here, we would also like to emphasize some considerations of privacy that are more ethical in nature, such as:

- The Data Protection Authority as a trusted social actor and role model in matters related to privacy and data protection and a pioneer in compliance with the GDPR
- The Data Protection Authority's own reputation and ethical standards
- The Data Protection Authority's presence on Facebook may be perceived as a guarantee for the platform's position on privacy and data protection
- We do *not* believe that the processing will have a deterring effect on the population.
- We do not know what potential data subjects or other interested parties outside of the Authority will think about this processing of personal data.
- We have reason to believe there will be several different and conflicting views on processing within the Authority.

Measures to minimize consequences to privacy:
The Data Protection Authority would be at the mercy of Facebook and its terms and conditions by creating and using a Page on the platform. This means we have no way of negotiating our own agreements with or in other ways influence Facebook's processing of personal data. At the same time, we must be aware that Facebook can, at any time, amend these terms and conditions. We can still emphasize certain key points and implement certain measures to improve the privacy terms:

- We could go further than most organizations in being open about our choice of communication platform and transparent about our assessments of the processing of personal data, as well as highlighting our own responsibilities as a result of communicating through a Page on Facebook. The most important information will be in place when we create a Page, and this information could be made available in the Page description ("About"), be included in a pinned post at the top of the Page, and be presented in a dedicate and more detailed statement on the Data Protection Authority website. There is, however, much we do not know about the processing.
- We should also be open about our channel concept and our practices for compliance with internal policies and moderation in our channel, so that this is predictable for our users. We should also make this known in-house.
- Making note of changes in Facebook's agreement/terms and conditions with Page owners, as well as defining and making note of any deviations. In addition, we should make note of negative media coverage and other types of negative publicity that concerns our presence on the platform.
- We could implement measures as described in the sub-chapter on information security in the systematic description of the data processing, such as good password hygiene and two-factor authentication.
- Not using Facebook plugins or similar tools on our own website. This is to minimize the amount of data collected outside of Facebook.

It is difficult to justify our own interest in using Facebook when we see the extensive processing of personal data it entails, as well as the limited opportunities the Data Protection Authority has to implement data protection measures.

Data protection principles

Fairness
The Data Protection Authority wants all data processing taking place on a Facebook Page to be fair and respecting of the data subject's interests and reasonable expectations. In addition, we want the processing to be transparent and understandable for the data subject, and not covert or manipulative. Measures like transparency about internal moderation policies and having a dedicated contact person will help in this regard. While the Data Protection Authority would like the processing to be fair, we are, nevertheless, largely at the mercy of Facebook.

The Working Party is uncertain if, and if so, to what degree, Facebook will process personal data with respect for the data subjects' interests, such as when the user is presented with content and advertising related to the digital profile Facebook has built about the user. In our assessment, the processing of the user's personal data may exceed the data subject's expectations, both in terms of specific types of communication on a Page and on the platform in general. Personal data collected by Facebook is used to make decisions about users and decisions that may affect users. Facebook's analyses, profiles and decisions are not particularly transparent,

and we are concerned that the profiling may be discriminatory and manipulative. It is, however, uncertain how much the Data Protection Authority's presence on the platform will contribute to this.

Transparency
The Data Protection Authority will provide information to the data subject. We are, however, concerned that the processing of personal data and clarifications of responsibilities may be characterized by a lack of transparency vis-à-vis Page owners and data subjects. Furthermore, it is reasonable to question the public documentation of Facebook's availability and completeness. The documentation seems complex and is characterized by inaccessible language and structure. After reading the documentation and attempting to prepare a complete systematic description of the data processing on the platform, there is still much we do not know about the processing. This is problematic from a privacy perspective.

Purpose limitation
We believe the Data Protection Authority's own purposes have been clearly specified and correspond well with the expectations of users in the context of following and interacting with a Page on Facebook.

On the part of Facebook, we believe the purposes are wide, vague and all-encompassing. For that reason, we believe it is difficult for users to know what their personal data is actually used for.

Data minimisation
We believe the purpose of processing can be achieved by limiting the collection of personal data, by using less detailed personal data, and by not using confidential or special categories of personal data. On the part of the Data Protection Authority, we believe data should be deleted as soon as it has served its purpose, e.g. after six months. We also believe that processing can be achieved by increased use of pseudonymous and/or aggregated personal data.

However, the Data Protection Authority cannot prevent users from stating and sharing what they want on the Page, nor is that the goal. We also have no influence over what Facebook collects in terms of the user's shared data, meta data, observation data and derived data when they interact with our Page. We believe that we also have no overview of the scope of Facebook's sharing of collected data with other parties.

We believe it is difficult to comply with the requirement of data minimisation in the context of a Page on Facebook. We believe this must be seen in light of the company's business model, which is to collect large and detailed quantities of data on Facebook users, which the company, in turn, may use for its own purposes.

Accuracy
When the Data Protection Authority posts information on our Page, we ensure that the information we post is accurate. Data subjects will be able to personally edit, update and delete their own posts and engagement. The Data Protection Authority will not be able to guarantee the accuracy of information posted by users. The moderator will also consider the users' posts in light of our own policies, and may, theoretically, delete posts that, for various reasons, are deemed "incorrect". Users may report posts they believe are incorrect and should be deleted, either to Facebook or to the owner of the Page.

To a certain extent, Facebook provides the user with control over which information they choose to share, they can report information posted by others, and they can object to certain types of processing. We would argue that some of the communication on the Page would be opinions, interpretations, etc. We therefore believe that it could be argued that the principle of accuracy is less relevant in the context of communicating through a Page on Facebook. As it is not clear which types of processing Facebook performs, it will, in practice, be difficult for the user to verify whether personal data is correct.[54]

Limitation of storage
The moderator will regularly delete information that is not relevant, that can be deemed offensive, or that includes special categories of personal data. The moderator will review all posts annually, and will normally delete all posts on the Page that are more than 5 years old. Dynamic content on the Page does not, in our view, have archival value, and will therefore not be archived outside of the platform.

Our assessment is that the extent to which Facebook deletes information on its own initiative, is unclear. Facebook writes that user information is deleted as soon

---

[54] See, e.g. the discussion in https://agendamagasin.no/kommentarer/tror-diskret-pa-nettet-tro-igjen/

as it is no longer necessary to provide services to the user, or when a user account is deleted.[55]

Integrity and confidentiality
In the *systematic description of the data processing* we presented our assessment of the data security of processing. We believe that Facebook wants and has implemented measures aimed at protecting its internal data security. We believe that certain risks to personal data security in the processing of information on the Page can be reduced to acceptable levels by implementing security measures.

Rights and freedoms of data subjects

Our options in terms of facilitating for and improving the rights and freedoms of the data subjects are minimal and largely at the mercy of Facebook. The Data Protection Authority's processing of personal data would, in our assessment, when viewed in isolation, not stand in the way of the data subject's right to non-discrimination, freedom of thought, conscience and religion, or freedom of expression and information. Regardless of the Data Protection Authority's procedures and efforts, we will not have any influence over Facebook's subsequent processing of personal data, and therefore we also have no influence over the processes that ultimately may lead to manipulation or discrimination, among other things.

We believe Facebook's information can be difficult to understand, and that most users may not fully understand the scope and consequences of this processing. More specifically, we believe that the information at times can be characterized by technical and legal jargon, as well as unclear and vague formulations, and it is difficult to navigate through the vast quantities of information. This also applies to rights, and we question whether these rights are actual and complete. We believe there is considerable room for improvement in the way Facebook handles the rights and freedoms of data subjects. Facebook's analyses, profiles and decisions are not particularly transparent, and we are concerned that the profiling may be both discriminatory and manipulative. It is, however, uncertain how much the Data Protection Authority's presence on the platform will contribute to this, and how much responsibility we have for this, cf. the assessment of joint controllership.

§ Article 25: Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

[55] https://www.facebook.com/privacy/explanation

Article 25 Data protection by design and by default

A data controller has an obligation to acquire, implement and maintain solutions, applications and tools that process personal data in accordance with the requirements of Article 25 of the GDPR on data protection by design and default.

The main principle of data protection by design and default is that these measures shall effectively implement and safeguard privacy principles and the rights and freedoms of data subjects in the processing performed by the solution used.

In our assessment of the necessity and proportionality of our use of a Page on Facebook, we consistently find that despite the Data Protection Authority's intention of protecting the principles of privacy and data protection and the rights and freedoms of data subjects, we are nevertheless at the mercy of Facebook and its terms and conditions by creating and using a Page on its platform.

Without going into the requirements of Article 25 in more detail, we question whether the personal data collected from a Page on Facebook will be processed in accordance with the requirements of data protection by default and by design.

Summary and assessment: necessity and proportionality

The objective of this chapter was to assess whether our processing activities are necessary and proportionate to the purposes.

- The Data Protection Authority's legal basis for creating and using a Page on Facebook is derived from Article 6 (1) (f) of the GDPR on the balancing of interests. The Working Party believes we have several legitimate interests for being present on the platform, and that the processing would have several positive outcomes for the data subject. The Working Party nevertheless believes that it is difficult to justify the Data Protection Authority's interests in using a Facebook Page when these interests are balanced against the processing of personal data.
- The Working Party believes the Data Protection Authority's own purposes have been clearly specified and correspond well with the expectations of users in the context of subscribing to and/or interacting with a Page on Facebook.
- The Working Party has identified measures for data minimisation in relation to the Data Protection Authority's purposes, when viewed in isolation, but the platform does not allow for the implementation of these measures.
- The Working Party believes the principle of accuracy is less relevant in our context of processing personal data through the use of a Facebook Page.
- The Data Protection Authority can edit and delete content at its discretion. It is unclear, however, whether the data is then also deleted from Facebook's underlying systems, or whether it remains there even after the Data Protection Authority has deleted it, and it is no longer visible to the user.

Despite the Data Protection Authority's intentions of protecting the legal basis, privacy principles and the rights and freedoms of data subjects, we would be at the mercy of Facebook and its terms and conditions by creating and using a page on the platform. This has the following implications:

- The Working Party believes Facebook's purposes can be seen as broad, vague and comprehensive. We believe it would be difficult for users to know what to expect from the processing.
- The Working Party's view is that we have no influence over what Facebook collects in terms of meta data, observational data and derived data when they interact with our Page.
- It will be difficult for users to verify that personal data is correct.
- The Working Party believes there are uncertainties associated with Facebook's actual storage periods.
- The Working Party believes there are several uncertainties associated with the way Facebook protects the rights and freedoms of data subjects. The Data Protection Authority has no influence over Facebook's processing of personal data, and consequently also has no influence over any processes that may put the data subject's rights and freedoms at risk.

Assessment of risks to the data subjects' rights and freedoms

So far in this report, we have assessed presence through a Page on Facebook from the perspective of the Data Protection Authority being a data controller with a wide range of obligations pursuant to the GDPR. In this chapter, we flip the perspective and look at the processing from the data subject's point of view, cf. the concepts in the figure below: transparency, predictability, co-determination, and trust (Norwegian).

Do we need a DPIA?

Article 35 of the GDPR provides that a data protection impact assessment (DPIA) must be carried out when a certain type of processing is likely to result in a high risk to the rights and freedoms of the data subject under the Regulation.

Based on the risks we identified in the systematic description in terms of the nature, scope, purpose and context of processing, and our conclusions in terms of necessity and proportionality, we have concluded that our use of Facebook as a communication platform would likely result in a high risk to the data subjects' rights and freedoms.

We also believe the processing fits several of the criteria of the Article 29 Working Party for evaluating when a DPIA is necessary,[56] as well as the Data Protection Authority's list of processing activities that always require a DPIA.[57]

Assessment of lack of true co-determination, transparency and predictability

Our DPIA is based on the above criteria, and we assess *true co-determination, true transparency, true predictability* in processing, to verify whether the processing can be performed in a manner that is acceptable to and builds trust with the data subject.

True co-determination
We primarily assess the degree of co-determination in light of the data subject's rights under the GDPR.

It is up to the individual to use Facebook as a platform for information and communication. The data subject personally makes the choice of creating a profile and is presented with the terms and conditions of the service when they create a profile on the platform.

It is also optional to subscribe to and interact with the Data Protection Authority's Page. Most of the information provided by the Data Protection Authority will already be publicly available and therefore not exclusively provided via Facebook. The discourse that emerges in communication with users, however, will be channel-specific.

The Data Protection Authority and its data protection officer (DPO) can help the data subject as much as we can by providing information and guidance in the exercise of their rights within the Facebook system. However, the Data Protection Authority is largely unable to actively help the data subject exercise other rights.

The Working Party has prepared a guide, which data subjects may use in their attempt to exercise their rights vis-à-vis Facebook.

---

[56] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10362

[57] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/

Within Facebook, the data subject has the right and the freedom, beyond information about their data, to access (access), correct (rectification), transfer (data portability), and delete their own data. By law, the data subject also has the right to oppose (object) and restrict certain types of processing of personal data. Among other things, this includes the right to object to the processing of data for direct marketing, the right to object to the processing of personal data where Facebook claims to be performing a task in the public interest or where Facebook is pursuing its own legitimate interest or the legitimate interest of a third party. A user may withdraw their consent for certain types of processing on Facebook, such as the processing of special categories of personal data, the use of location data or the use of facial recognition. A user may at any time choose to delete their Facebook account.

The data subject may contact Facebook via a contact form, via mail or through a dedicated data protection officer with Facebook Ireland Ltd. The data subject may also file a complaint with Facebook Ireland's supervisory authority, the Irish Data Protection Commission, or through the Norwegian supervisory authority.

It has already been pointed out that, in the Working Party's assessment, there are several uncertainties associated with the true opportunity to exercise these rights, e.g. related to the completeness of access to the user's own data or a demand for permanent erasure of personal data. The nature of the platform means that a data subject would only, to a very limited degree, be able to exercise their rights vis-à-vis a specific Page on the platform.

The data subject would furthermore have some degree of choice through the platform's functionality, such as the editing and deleting of something they actively have shared on a Facebook Page. Nevertheless, the Working Party's remains that the data subject will have limited choice, limited options for reservations and limited true co-determination in a wide range of processing, including processing related to a specific Facebook Page, such as:

- Which types of personal data are collected, and the use of various sources.
- The volume of personal data.
- What constitutes a basis for assessment or evaluation of the data subject.
- Storage period.
- Geographical scope of storage
- Decisions about the data subject based on systematic and comprehensive analyses of personal data.
- Use of personal data for new or different purposes.
- Limited control over data flows, processing chains or disclosure to third parties.

We believe that having the opportunity to exercise one's rights pursuant to the GDPR strengthens the data subject's choice and co-determination. The Data Protection Authority is, however, at the mercy of how Facebook chooses to allow users to influence and control the processing of their personal data and the degree to which users are allowed to exercise their rights and freedoms.

True transparency.
Facebook describes the processing of personal data in its privacy policy, as well as in a wide range of other publicly available documents on the platform. Nevertheless, we question whether Facebook is sufficiently transparent about:

- Safeguarding of privacy principles
- The complexity of processing
- Regular and systematic processing
- To whom Facebook discloses data, general data flows, software and algorithms used, and how decisions are made
- The chain of processing activities
- How much data Facebook actually has in its possession, and how this data may be used to influence the user
- The basis for assessment or evaluation of the data subject
- The extent and scope of processing
- Matching or linking data sets from different sources

We also question whether Facebook is sufficiently transparent about arrangements for joint controllership with Page owners. This contributes to ambiguity in terms of responsibilities vis-à-vis Page owners and individual users.

The threat associated with a potential lack of transparency on Facebook's part may be that Facebook may hide illegitimate processing behind unclear, unintelligible and incomplete information. This could entail that the data subjects do not have sufficient information to make good choices in their presence on the platform, or they may be ignorant to the basis on which certain decisions that affect them were made. Inaccessible information may potentially lead to the data

subject being unable to exercise their rights pursuant to the GDPR. In a situation where one party knows much more about the other party, there will also be an unequal power balance.

We believe that the Data Protection Authority's presence on Facebook, through a Page, would not, when viewed in isolation, worsen or in other ways affect the degree of transparency vis-à-vis the data subject on the platform. However, as a data controller, we are, in this context, too, at the mercy of Facebook and the extent to which Facebook chooses to be transparent about its processing activities and what they choose to provide the data subjects information about and access to.

True predictability
Facebook will process personal data generated on the Data Protection Authority's Facebook Page for its own purposes, which will likely be unpredictable for the data subject. We believe Facebook's processing of personal data is unpredictable in several different ways, such as:

- Profiling, automated decision-making and decisions based on systematic and comprehensive analyses
- The basis for assessment or evaluation of the data subject
- The data subject's expectation of confidentiality and privacy in certain types of communication on the platform
- Storage periods and whether erasure of personal data is permanent
- The volume of personal data linked to individuals and what this may entail
- Potential use of special categories of personal data
- Matching or linking data sets from different sources
- Facebook uses evolving and innovative technology, which entails new types of processing
- Facebook can at any time choose to amend their terms and conditions. Data subjects and/or Page owners will however be notified of any significant changes.

The complexity of Facebook's processing will, in our assessment, be so comprehensive that the data subject in many cases will not know what to expect. The processing may have unpredictable consequences and may lead to unpredictable decision-making in the user experience.

The Working Party's view is that the Data Protection Authority's Page on Facebook, when viewed in isolation, largely would not conflict with the data subjects' expectations. The Working Party believes that the Data Protection Authority's processing in accordance with its own defined purposes could be perceived as limited in scope, clear, predictable and professional. Most Facebook users will be used to communicating with Pages, and as such, these types of processing may be perceived as predictable for the data subject. We are, however, at the mercy of Facebook in how they choose to process personal data for its own purposes and the degree to which they choose to be transparent about their processing in order for the data subjects to perceive them as predictable.

What can we do to build trust?
In order to build trust in data subjects, the Working Party proposed the following measures:

- Consider making the risk assessment of Facebook available on request or consider proactively communicating this work, ref. the ombudsman role.
- Refer to surveys, reports, research, etc. on Facebook and social media
- Monitor Facebook's policies/terms and conditions for changes and regularly assess risks
- Monitor the media for privacy related coverage of Facebook
- Monitor other European data protection authorities for how they approach the use of Facebook and other social media
- Obtain the data subjects'/representatives of the data subjects' views on the processing.

Note! Even though consulting with the DPO and management validation of the DPIA are requirements under the GDPR, they may still be considered trust-building measures.

Memo from the DPO

Our data protection officer gave his assessments and views based on a previous version of the report, which was presented to management. The DPO's considerations have been included in this version.

Summary and assessment: Assessment of risks to the data subjects' rights and freedoms

We believe a DPIA was necessary due to the following:

- The processing intersects with several of the Article 29 group's criteria.

- The processing intersects with the criteria on the Data Protection Authority's own DPIA list.

This means we must assess true co-determination, true transparency and true predictability in processing. In these areas, we concluded as follows:

- The data subject will have a *lack of choice and lack of true co-determination* in a wide range of processing types, such as the types of personal data collected, how the data is used or stored, and the geographical scope of storage. This threatens several of the data subject's rights and freedoms. The lack of co-determination also includes processing related to one specific Facebook Page.
- We question whether Facebook is *sufficiently transparent* about such things as its algorithm and the complexity of processing, disclosure of personal data and data set matching. This could threaten and have multiple implications for the data subject's rights and freedoms, such as the data subjects not exercising their rights under the GDPR. We also question whether Facebook is sufficiently clear about is responsibilities vis-à-vis users or Page owners.
- We believe *Facebook's processing can be unpredictable* in several ways, e.g. in connection with profiling and automated decision-making, expectations of confidentiality, data set matching or use of new and innovative technology. Facebook can at any time choose to amend their terms and conditions. The processing can have unpredictable outcomes for the data subjects. We believe interaction with Pages on Facebook, when viewed in isolation, would appear to be predictable.
- We can implement some other trust-building measures beyond those described in the assessment of necessity and proportionality.

In general, we are at the mercy of how Facebook chooses to process personal data for its purposes. We are also at the mercy of the degree to which Facebook chooses to provide its users with true choice, and how predictable and transparent about its processing Facebook chooses to be with its users.

We believe the high risks to the data subjects' rights and freedoms would still remain after implementation of these proposed measures.

Validation from Management Team

Figure "Management Team validation of DPIA": Compile and present findings; Considerations of stakeholders; Review, decision and approval.

We believe that this report has provided the Management Team with sufficient information on which to make a decision. Particularly in consideration of the DPIA and considerations of relevant stakeholders, the Management Team is asked to decide on one of the following:

1. We implement a Facebook Page as a communication platform. This entails that the Management Team does not find that the processing of personal data entails a high risk to the rights and freedoms of data subjects.
2. Conditional upon improvements in the assessment. The Management Team provides clarification on what requires improvement, and the Working Party will come back with a revised DPIA and presents this to the Management Team.
3. Rejected: The Management Team decides not to go through with personal data processing through a Facebook Page.
4. If the Management Team decides to proceed, and the report has been reviewed by the Management Team more than once, but the risk to the data subject's rights and freedoms is too high (and we are unable to mitigate it), the Management Team (Data Protection Authority) will ask for a preliminary consultation with a substitute data protection authority.

Conclusions and recommendations of the Working Party

In an assessment of the presence and role of a public body, such as the Data Protection Authority, on a social medium, the democratic perspective cannot be underestimated. Facebook doubtless has considerable potential as an information and communication channel for important target audiences and the wider population.

The benefits of social media must be weighed against their drawbacks, however. Despite the communicative objectives of being present on a platform where many potential users and audiences already are, we recommend that the Data Protection Authority not implement use of Facebook.

After performing a structured assessment, our conclusion is relatively clear. First, we believe that the processing of personal data carries a high risk to the rights and freedoms of data subjects (1). We do not see how a revised DPIA can change that fact (2). We recommend that the Management Team not go through with personal data processing through a Facebook Page (3). A preliminary consultation with a substitute data protection authority should not be relevant if the recommendations above are applied (4).

In addition, we believe that a presence on Facebook and the company's subsequent processing of personal data would have considerable impact on the Data Protection Authority's reputation and ethical standards. We believe that the Data Protection Authority's decision on whether or not to implement Facebook will be noticed, and it may have an impact on the use of the platform by other parties. Consequently, the circle of data subjects affected by the Data Protection Authority's decision could extend beyond those who would choose to use the Data Protection Authority's Page. We believe that the Data Protection Authority, by its very nature, should attach considerable importance to its position as a role model in privacy matters. If the Data Protection Authority joins Facebook, it could help legitimize the use by

organizations of a platform that may pose a high risk to the rights and freedoms of data subjects.

Notwithstanding, it is the recommendation of the Working Party to consider other social media platforms to safeguard professional and active communication, ensure high effectiveness for our activities and interact with the public in a way they are used to and in a way they like.

The Management Team's decision

In a Management Team meeting on 03/03/2020, the executive group agreed with the recommendations from the Working Party, with some minor changes. These changes are reflected in this version of the report.

Appendix 1 — Assessment of joint controllership

In this assessment, it is especially important to clarify the roles and responsibilities of the Data Protection Authority and Facebook, respectively, in data processing.

What is joint controllership? The GDPR provides that two or more data controllers may have joint controllership.

Joint controllership occurs when two or more separate data controllers jointly determine the purposes and means of processing, or when their decisions concerning purpose and means of processing converge. Joint controllership does not occur when several data controllers separately make decisions concerning purposes and means, even if the controllers process the same personal data.

Each data controller needs a legal basis for its processing of personal data. Data controllers must establish an arrangement that, in a transparent manner, determines their respective responsibilities for compliance with the provisions of the Regulation, as well as the controllers' roles and responsibilities vis-a-vis the data subjects. The European Data Protection Board (EDPB) has issued guidelines on the concepts of controller and processor.[58] These guidelines specify that both data controllers are ultimately responsible for the processing overall, even if they have distributed responsibilities among themselves in an arrangement.

The European Court of Justice has ruled that joint controllership between two parties does not entail that one controller is responsible for prior or subsequent processing, where the other party solely determines the purpose and the means.[59] In practice, it can be difficult to draw the line between processing activities and determine where joint controllership "begins" and "ends".

European Court of Justice ruling in C-210/16 Wirtschaftsakademie

In its ruling in the so-called Wirtschaftsakademie[60] case, the European Court of Justice found that an administrator of a Page ("fan page") on Facebook could be considered a data controller under the Data

§ Article 26: Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

[58] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[59] C-40/17 *Fashion ID* para. 74.

[60] C-210/16 *Wirtschaftsakademie*

Protection Directive in force at the time,[61] for the collection of personal data about individuals who visit the Page. This ruling is relevant even under the current GDPR. It is worth noting that Facebook and Wirtschaftsakademie in part had different purposes for the collection of data. The court pointed out that Facebook and the administrator do not necessarily have equal responsibility, even though they have a joint responsibility, and that the level of responsibility would be dependent on the degree to which each of the two operators are involved in the processing.[62]

European Court of Justice ruling C-40/17 Fashion ID

In its ruling in the so-called Fashion ID[63] case, the European Court of Justice gave its opinion on joint controllership. This ruling concerned the interpretation of provisions in the Data Protection Directive, which was in force at the time, but like the Wirtschaftsakademie judgment, this will be relevant in the interpretation of the current GDPR.

Fashion ID involves an online shop, which had included the Facebook "like" button on its website. Through this "like" button, information about visitors to the website was collected and shared with Facebook, even without the visitors clicking on or on other ways interacting with the "like" button.

In its Fashion ID ruling, the European Court of Justice found that the online shop and Facebook were joint controllers of the processing activity, which consisted of collecting and sharing with Facebook information about visitors to the website ("*collection and disclosure by transmission*").[64] The reasoning behind this was that in this processing activity, the online shop and Facebook jointly determined the purpose and means of processing. Facebook and Fashion ID had different purposes for the processing activity, but it was performed in pursuit of their joint economic interest.

The Court furthermore points out that Facebook would not have had access to personal data about visitors to the site without the online shop making the "like" button part of its website. Therefore, the online shop "*exerts a decisive influence*" over the collection of personal data.[65] The court also found that the two operators have joint controllership, even if the online shop did not have access to the personal data collected.[66]

Description of processing activities for which the Data Protection Authority and Facebook would have joint controllership

It is difficult to define the limits of the processing for which Facebook and the Data Protection Authority would have joint controllership. Based on our mapping, Facebook processes personal data for a wide range of purposes that go far beyond the purposes for which the Data Protection Authority will process personal data. In our view, several of Facebook's purposes are vaguely defined and unclear. The question is whether the Data Protection Authority could be considered to have joint controllership with Facebook even for processing that primarily involves Facebook, and that is performed in pursuit of purposes defined solely by Facebook.

The Fashion ID ruling makes it clear that the two operators have joint controllership of the collection from Fashion ID's website and the disclosure of personal data from Fashion ID to Facebook, even though the operators have different purposes for the processing. At the same time, the ruling also makes it clear that the online shop does not have joint controllership with Facebook for any subsequent processing Facebook may perform, even if the operators have joint controllership for the collection of personal data itself.

In other words: The Data Protection Authority may be joint controller of processing activities we contribute to and enable, even though Facebook's purpose for the activity differs from ours. That does not mean our level of responsibility is equal; it is possible to have unequal levels of responsibility. We are, however, not responsible for any subsequent processing by Facebook we do not contribute to.

On this basis, there will be a limit to the processing activity for which the Data Protection Authority and Facebook have joint controllership. If we follow the logic of the Fashion ID ruling, the Data Protection Authority would not have joint controllership with Facebook of all

---

[61] This refers to the data protection legislation in force prior to May 2018, the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

[62] C-210/16 *Wirtschaftsakademie* para. 43.

[63] C-40/17 *Fashion ID*.

[64] *Ibid.* para. 76.

[65] *Ibid.* para. 78.

[66] *Ibid.* para 82.

of Facebook's subsequent processing. Would it, in theory, be possible to define a limit for when the Data Protection Authority and Facebook no longer jointly determine the purpose and means of the processing of personal data? We believe it is difficult to define exactly where to draw this line.

With consideration of principles of accountability, transparency and predictability, one could argue that the Data Protection Authority, from an ethical perspective, could be responsible for Facebook's subsequent processing. This is because the Data Protection Authority, by having a Page, contributes to the collection of personal data, which in turn is used and processed by Facebook in a way we believe may pose a risk to the rights and freedoms of data subject.

Considerations of the data subject being in control of their personal data also point in this direction. This is personal data Facebook would not have had access to without the Data Protection Authority's actions, see also the reasoning in Fashion ID para. 78. The question of (joint) controllership notwithstanding, our assessment is that this subsequent processing by Facebook is relevant for the Data Protection Authority's obligation to provide information pursuant to Articles 5, 12, 13 and 14.

While the boundaries are unclear, we believe, at the very least, that the following processing activities *may* be included in a joint controllership with Facebook.

- The Data Protection Authority and Facebook would be joint controllers of the collection of personal data about users visiting or interacting with the Data Protection Authority's Facebook Page.
- The Data Protection Authority and Facebook would be joint controllers of outcome of the analysis of personal data about users visiting or interacting with the Data Protection Authority's Facebook Page ("Page Insights").
- We are uncertain whether the Data Protection Authority will have some level of joint controllership for Facebook's use of personal data about users visiting the Data Protection Authority's Facebook Page to enrich user profiles for the purpose of providing personalized advertising.

In addition, we believe that:

- The Data Protection Authority and Facebook share a joint responsibility for informing users, in a transparent, accessible and understandable way, of what their personal data will be used for.
- Facebook and the Data Protection Authority have a joint responsibility for protecting the rights and freedoms of data subjects.

Facebook's joint controllership arrangement is problematic

Facebook has established a *joint controllership arrangement* called the *Page Insights Addendum*,[67] which is part of Facebook's terms and conditions.

The Data Protection Authority will not be able to negotiate a separate agreement or arrangement with Facebook concerning joint controllership. Consequently, the Data Protection Authority must assess whether the terms and conditions presented by Facebook are acceptable. Whether or not the arrangement is deemed acceptable would depend both on whether the Data Protection Authority finds (1) that the arrangement covers all processing for which the parties have joint controllership; (2) that the Data Protection Authority, by entering into the arrangement fulfils the requirements of Article 26 of the GDPR; and (3) that the terms and conditions of the arrangements are acceptable to the Data Protection Authority.

According to the arrangement, it applies to the joint controllership of the operators for aggregated statistics created from events logged by Facebook servers when people interact with a Page and the content associated with a Page. The arrangement stipulates that only Facebook has access to the underlying personal data and the events on which the insights are based. A Page administrator, like the Data Protection Authority, would only have access to the aggregated analysis provided by Facebook ("*Page Insights*").

The arrangement stipulates that events that form the basis for insights, may also be associated with individuals who are not logged in as Facebook users. This would occur if the individuals visit a site or click on a photo or video in a post to view it.

This arrangement, *Page Insights Addendum* is the only arrangement Facebook has made concerning joint controllership. In our assessment, it is uncertain

[67] https://www.facebook.com/legal/terms/page_controller_addendum

whether the arrangement covers processing activities for which we consider Facebook and the Data Protection Authority to have joint controllership. This relationship is made even more complicated by the fact that it is also difficult to define the limits for the joint controllership.

As for the specific terms of the arrangement, we would like to emphasize some main points: The arrangement is dynamic; Facebook can amend the arrangement whenever it wants, and Facebook may not necessarily give notice of amendments to the arrangement. The Data Protection Authority's only option if the Authority deems any amendments to the arrangement unacceptable, would be to terminate its use of the Page. In our understanding, the arrangement does not grant us the right to demand that personal data already collected be deleted. By accepting the arrangement, the Data Protection Authority accepts that any and all disputes between the Data Protection Authority and Facebook be settled by Irish courts under Irish law — the Data Protection Authority's legal position in a potential dispute is therefore unclear to us.

Review of Article 26 (1), (2) and (3)

Purpose and interests
The Data Protection Authority's purposes are generally different from Facebook's purposes. Facebook's main purpose is to "Give people the power to build community and bring the world closer together" as well as a wide range of other purposes listed in Facebook's Data Policy.[68] The Data Protection Authority's purpose is public education and discourse on data protection. Facebook's purpose is so wide that it would necessarily encompass the Data Protection Authority's purpose. Our joint interest is to reach a wide community with our message and to engage Facebook users, as well as to measure and analyse traffic/content on the Page.

Means
In order for the Data Protection Authority to achieve its stated purpose, the Data Protection Authority wants to use a Page on Facebook as the means, i.e. its communication platform. Under Article 25, the data controller is obligated to use solutions that have data protection by design and by default. We question whether the personal data collected from Pages on Facebook will be processed in accordance with this requirement, ref. the chapter on necessity and proportionality. Therefore, it is uncertain whether we will be in compliance with this obligation, given the responsibility we may have in this relationship.

Responsibilities, obligations, information and point of contact (cf. Article 26 (1)
Article 26 provides that responsibilities must be determined/clarified. Our assessment indicates that it is unclear what the limits are for processing activities where the Data Protection Authority and Facebook have joint controllership and activities where the Data Protection Authority and Facebook have separate controllerships.

Furthermore, it is also unclear which type of processing Facebook performs with personal data generated from the Data Protection Authority's Page. Through its Facebook Page, the Data Protection Authority contributes to the collection of personal data. This personal data may subsequently be used by Facebook in other processing activities. Given that Facebook's subsequent processing activities are so unknown and unclear to us, it is difficult for the Data Protection Authority to act in accordance with its responsibilities. Again: It is difficult to determine where the Data Protection Authority's responsibility "begins" and "ends". It is therefore difficult to fulfil the requirement of determining the *respective responsibilities* of the operators pursuant to Article 26.

The extent to which the Data Protection Authority is able to fulfil its *obligations* pursuant to the GDPR is unclear, especially that of the data subjects' true opportunity to exercise their rights. The data subject would largely be dependent on having to contact Facebook to exercise a right. If Facebook fails to respond or does not comply with the data subject's request, the Data Protection Authority will have limited opportunities to help the data subject. We believe the obligation to *provide information* pursuant to Articles 13 and 14 can be fulfilled by both Facebook and the Data Protection Authority.

A point of contact for the data subjects has been established by Facebook and will be established by the Data Protection Authority, in accordance with Article 26 (1).

[68] https://www.facebook.com/about/privacy/update

Our assessment is that the Data Protection Authority only partially fulfils its obligations pursuant to Article 26 (1) of the GDPR.

Arrangement (cf. Article 26 (2))
The joint controllership arrangement is unclear and can be amended by Facebook at any time.

The joint controllership arrangement was prepared by Facebook and only applies to measurements and analyses ("Insights"). It is our assessment that the joint controllership is broader than this arrangement. This means we lack arrangements for the other types of processing performed. The roles and responsibilities for activities not covered by this arrangement have not been defined.

The Insights arrangements is available on Facebook's website and is accessible to the data subjects. We believe it is unlikely that we will be able to establish an arrangement for other processing activities. A potential arrangement of this sort would be further complicated by the fact that it is difficult to define limits for the joint controllership.

Our assessment is that the Data Protection Authority only partially fulfils its obligations pursuant to Article 26 (2) of the GDPR.

Arrangement for exercising rights against the individual data controller (cf. Article 26 (3)
The data subject will only to a limited degree be able to exercise their rights against the Data Protection Authority. The data subject's other rights must be exercised against Facebook.

Our assessment is that the Data Protection Authority is not able to fulfil its obligations pursuant to Article 26 (3) of the GDPR.

Appendix 2 — Assessment of personal data security

In this description, we assess whether personal data security/information security is sufficiently protected pursuant to Article 32.

Information security risk is defined as the correlation between the following three factors:

1. **Value assessment**, i.e. classification of the information/personal data (value)
2. **Threat assessment** — threats and threat agents that pose a risk to our values
3. **Vulnerability assessment** — how vulnerable are we, and where are our vulnerabilities, given our values and the threats to our values

Value assessment: Data protection legislation defines personal data as a value. By communicating through a Page on Facebook, the Data Protection Authority will generate personal data. We have chosen to split and define the values (personal data) processed by Facebook into two: We distinguish between *"Public information"* in accordance with purpose 1 and *"Communication with users"* in accordance with purpose 2.

The *Public information* value is the information the Data Protection Authority chooses to post on its Facebook Page. This includes, among other things, information from our website, news, guides, blog posts, sharing of other pages'/organizations' content (curated content), videos, live streams, images, graphics and links. Based on this information, we have assessed our requirements for confidentiality, integrity and accessibility as follows:

Total confidentiality	Low
Total integrity	High
Total accessibility	Low

Our assessment indicates that it would not be a problem if the information we post is spread (confidentiality of the information), because that is the purpose of using a Facebook page. The accessibility characteristic is also found to be low. This means that if the information we post on our Facebook Page disappears or is lost, this would not be a major problem for the Data Protection Authority. Our primary channel will remain www.datatilsynet.no, and we manage several other channels (data protection blog, newsletter, Twitter). The most important security characteristic of the *public information* is, in our assessment, integrity. It is of considerable interest to us to make sure that what we post is correct and cannot be changed by unauthorized parties.

The value *Communication with users* encompasses all information that makes up the dialogue between users and the Data Protection Authority on our Page, and includes comments, direct messages, shared posts and engagement. By nature of the Facebook platform, which is a profile-based medium, statements and engagement will directly generate a wide range of personal data as a result of users interacting with the Data Protection Authority's Page on Facebook. We have assessed our requirements for confidentiality, integrity and accessibility as follows:

Total confidentiality	Very high
Total integrity	High
Total accessibility	Low

Based on what we know from our guidance activities and other contact with the public, we believe special categories of personal data could be posted on the Data Protection Authority's Page on Facebook, for example by vulnerable users or users who do not understand the full extent to which they are sharing information about themselves and others. That is why we have assessed the confidentiality requirement for the communication with users as very high. This also entails that we must be able to delete unwanted information, such as inappropriate, discriminatory or harassing comments and special categories of personal data posted by users, either about themselves or somebody else. Furthermore, it is our assessment that the integrity requirement should be high. This indicates that we presume users deem it important that nobody be able to change or manipulate their statements, comments or other engagement in their communication with our Page. As for the accessibility of the information, our assessment indicates that it would not be significant if the dialogue with users were to be lost. This could potentially be seen as somewhat annoying for some users, but we nevertheless assess this to be low.

Threat assessment: In the threat assessment, we consider relevant threats and threat agents. These have the potential, consciously or unconsciously, to harm our

Threat agent	Intention	Attack vector/threat
Ordinary users/children/incompetent users	No malicious intent, but may interact with the Page without understanding the consequences.	Via comments, DMs, etc., making available their own or others' (special categories of) personal data
Mentally unstable individuals	Revenge, frustration, desperation, demonstration	Via comments, DMs, etc., making available their own or others' (special categories of) personal data
Activists/online activists	Intending to undermine the Authority's authority or reputation, Authority employees or members of the public	Compromised: access to user accounts with Data Protection Authority moderator rights Changing information or posts on the Authority's Page
Trolls	Intending to provoke, distract, polarize and undermine	Posting large quantities of criticism and spam/irrelevant content on the Authority's Page
Insiders/Authority employees	Could post personal data without clearing this with the data subject. No malicious intent, but could act without understanding the consequences.	By posting Has administrator access to perform operations or change settings on the Page.

values, i.e. the personal data identified in the value assessment above, which the Data Protection Authority will be managing through a Page on Facebook. In the table above, we describe some central threat agents, as well as their presumed intention and attack vector:

Vulnerability assessment: A vulnerability assessment is needed to identify which risk-mitigating measures are necessary. Given our values and identified threats/threat agents: how vulnerable is the Data Protection Authority, and where are our vulnerabilities in terms of these attack vectors?

When assessing for vulnerabilities, one must begin with checking various security standards. These checks help reveal whether we are vulnerable to known threats and set a minimum standard for vulnerability-mitigating measures.

The vulnerabilities in the table below largely reflect the vulnerabilities the Data Protection Authority will be in a position to do anything about.

The Data Protection Authority operates with the following four risk levels: LOW, MODERATE, HIGH and VERY HIGH.

No.	Vulnerability	Risk level
1	We are at the mercy of Facebook's terms and conditions for data processing, and as data controllers, we cannot make information security demands on our processor and/or joint controller.	HIGH
2	The Data Protection Authority posts personal data without sufficient clarification or legal basis.	LOW
3	Free text in posts or comments	HIGH
4	Users may spread personal data outside the Page, either on or outside the platform	HIGH
5	Lack of control of the Page's information and communication flows and of the life of the information	MODERATE
6	Lack of procedures and policies within the Data Protection Authority for Page moderation	LOW
7	Unclear distribution of responsibilities for the Facebook	LOW

	Page within the Data Protection Authority	
8	Lack of/poor access control and authentication	MODERATE
9	Access management and erasure within Facebook	HIGH
10	Lack of control over ICT devices used by moderators/administrators	LOW

Risks to personal data security, vulnerability-mitigating measures and residual risk

The numbers in column 1 correspond to the vulnerabilities identified in the table in the previous section. The table below shows risks before and after implementation of vulnerability-mitigating measures.

No.	Risk level	Vulnerability-mitigating measure	Residual risk
1	HIGH	No measures	HIGH
2	LOW	The Data Protection Authority must establish procedures and roles for publication.	LOW
3	HIGH	Control after-the-fact only: Moderate, i.e. hide/delete posts. Activate “profanity filter”.	HIGH
4	HIGH	Delete posts ASAP from the Page (moderation and follow-up). Users will still have a window where they are able to share the post beyond the Page.	HIGH
5	MODERATE	Determine responsibilities and establish moderation procedures.	LOW
6	LOW	Define and document the use of Facebook through org. measures: policies, training, etc. Our control system includes guidelines for use of the Page.	LOW
7	LOW	Our control system includes guidelines for use of a Facebook Page.	LOW
		Determine responsibilities and establish moderation procedures. Define and document use of the platform. Determine and review roles, including resource allocation.	
8	MODERATE	Dedicated user for Page moderation and administration only. Password hygiene. Activate two-factor authentication. Define roles and user types. Regular access audits.	LOW
9	HIGH	We have no way of instructing Facebook on access to and deletion of “our” personal data.	HIGH
10	LOW	Mobile Device Management. Password hygiene.	LOW

Office address:
Trelastgata 3, 0191 Oslo

Postal address:
Postboks 458 Sentrum
0105 Oslo, Norway

postkasse@datatilsynet.no
Telephone: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no
twitter.com/datatilsynet