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

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 organization'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. This version of the report briefly summarizes our analyses, assessments and conclusions concerning risks, risk management and duties 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 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. The English version of the report has not been supplemented with clarifications, nor taken into account or addressed key developments in the field of privacy after this.

This report is a an abridged version of the Norwegian report.

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 this assessment, our capacity 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. Our assessment of Facebook is therefore primarily our organization's own assessment of what it would entail, in terms of accountability, to create a Page on Facebook, and of whether we would be compliant with relevant privacy laws.

In making sure the privacy of data subjects registered in a solution is protected, a Data Protection Impact Assessment (DPIA) is an important tool. This report addresses the risks and risk management associated with creating and communicating through a Page on Facebook. It presents a systematic description of the solution, a legal assessment of accountability, an assessment of the necessity and proportionality of processing, and considers measures to reduce privacy risks for the data subjects registered in the solution. The report also addresses ethical considerations in light of the Data Protection Authority's values[1] and the Authority's position as a role model in privacy issues.

Conclusion

This report was finalized by the Management Team. Based on this report and the recommendations of the Working Party, the Data Protection Authority has decided *not* to create and communicate through a Page on Facebook.

The Management Team agreed with the recommendations provided in the submitted report, with some amendments. This report includes changes based on discussions in Management Team meetings, as well as discussions in the organization's wider management meeting, including the final conclusion. 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 processing of personal data through a Page on Facebook are too high.
- The Working Party believe that the Data Protection Authority will 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 believes that it is not sufficient for The Data Protection Authority to enter into Facebook standard agreement with Facebook 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 will probably not be possible for the Data Protection Authority to comly with the requirements of Article 25 of the GDPR on data protection by design and by default setting if we use Facebook.
- The Authority's data protection officer recommends that the Data Protection Authority not implement Facebook as a communication platform.

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

- The Working Party finds that the Data Protection Authority should place considerable emphasis on its position as a role model and compliance with relevant privacy laws.

Brief analyses, assessments and recommendations of the Working Party have been summarized in this report. This report is an abridged version of the Norwegian report.

Facebook and communication

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 an account 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 media 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 target groups 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 have therefore not been discussed in this report.

Risk assessment

The assessment should provide the 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, a Working Party, comprised of experts in law, technology and media.

The mapping and analysis are primarily based on Facebook's privacy policy[2] and other material made available by Facebook. This analysis material has been collected in the period July 2019 up to and including 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 arrangements with joint controllers.

Parties and roles

This assessment seeks to clarify roles and responsibilities. In using Facebook, there will be several types of parties involved: the provider (Facebook), the Page owner (Data Protection Authority), users (data subjects) and other parties (e.g. advertisers, subcontractors and Facebook's partners). In this assessment, we have emphasized clarifying the roles and responsibilities of the Data Protection Authority and Facebook, respectively, in data processing.

Execution

In this assessment, we have applied the Data Protection Authority's own templates for risk assessments and DPIAs. This template serves 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 this report based on a procedure developed by the Data Protection Authority itself.[3] 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 began by preparing a *systematic description of the data processing*[4] associated with having a Page on Facebook. 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. We also assess our compliance with the provisions concerning joint controllership with Facebook pursuant to Article 26 of the GDPR.

We then assessed the *necessity and proportionality of the data processing*[5]. 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. We also briefly accounted for whether the use of a Page on Facebook is in compliance with the principle of data protection by design and by default under Article 25.

The focus is on the obligations of the Data Protection Authority pursuant to the GDPR. We did find, however, considerable risks to the data subject's rights and freedoms. We have therefore performed a data protection impact assessment (DPIA) pursuant to Article 35 of the Regulation, where we flip the perspective and consider whether the data processing should take place, from the data subject's perspective. The Working Party has consulted with the Data Protection Authority's data protection officer (DPO) in accordance with Article 35 (2).

---

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

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

[4] The descriptions are seen in light of Articles 24, 30 and 32 of the GDPR.

[5] Seen in light of the privacy principles of Articles 5, 6, and 9 of the GDPR, the rights of data subjects in Article 22-22 of the Regulation, and the freedoms of the data subject pursuant to the fourth preamble to the Regulation and Article 8 of the ECHR.

Systematic description of the data processing

We prepared a systematic description of the data processing of personal data associated with creating and communicating through a Page on Facebook.

Nature, scope, purpose and context

By considering the nature, scope, purpose and context of data processing, we identify risks to the data subject's privacy, rights and freedoms.[6] We have summarized the risks and the Working Party's assessments of these risks below:

The Working Party's assessment is that the following risks is associated with the nature of processing:

- Believe it is difficult for the data subject to exercise their rights pursuant to the GDPR vis-à-vis Facebook
- Believe that the processing of personal data is characterized by unpredictability
- Believe that the processing of personal data is characterized by a lack of transparency vis-à-vis the data subject
- Believe that there are uncertainties associated with the protection of several privacy principles
- Our communication on a Page would entail systematic processing, in the form of profiling and automated decision-making
- Believe that the potential of an unequal power balance between the company and the user may be problematic
- Believe that this processing involves innovative technology that is constantly evolving

The Working Party's assessment is that the following risks is associated with the scope of processing:

- Processing will include many different categories of personal data, including special categories of data.
- The processing potentially entails processing of personal data concerning vulnerable persons.
- The processing includes a large number of data subjects.
- The volume of personal data about the data subject is large and detailed.
- Uncertainties concerning storage periods, including potentially permanent storage.
- The geographical scope of storage is global, which includes areas outside the EU/EEA.

The Working Party's assessment is that the following risks is associated with the purpose of processing:

- Believe Facebook's purposes to be vague, ambiguous and extensive, and that they, to a large extent, diverge from the purposes the Data Protection Authority have defined for the data processing.
- Believe there are uncertainties about whether personal data will be used for new or alternative purposes.
- Believe that decisions made about the data subject may have consequences for the data subject.
- Believe that decisions are made about the data subject based on systematic and comprehensive analyses of personal data.

The Working Party's assessment is that the following risks is associated with the context of processing:

- Believe that there are uncertainties associated with sources, data sets, and compilations of data sets within and outside of the platform.
- Believe that the data subjects could have an expectation of confidentiality and privacy in certain types of communication with a Page on the platform.
- Believe that it could be difficult for the data subject to stay informed and in control of their own data.
- Believe that data flows and chains of processing seem unclear, including who the recipients of personal data are.

Information security

Further, the Working Party have summarized an assessment of whether the processing protects data security:

- In our 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. Objective 1) on the Page is "high". We also concluded that our requirements for confidentiality

[6] In the analysis, we have tried to distinguish between the Data Protection Authority's processing activities in connection with communication through a Page on the platform and Facebook's processing activities for its own purposes.

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. Objective 2)*.
- In our threat assessment, we have identified and described a selection of what we consider to be the most relevant threats and threat actors: including ordinary users, children, mentally unstable persons, online activists, online trolls and Data Protection Authority employees.
- In our vulnerability assessment, we have described our presumed vulnerabilities in relation to processing, including, e.g., posting without clarification, lack of control over comments and the information flow of the Page and 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.

Assessment of joint controllership
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 come to the following conclusion:

- The Data Protection Authority has joint controllership with Facebook if the Authority creates a Page on Facebook, ref. the Fashion ID[7] and Wirtschaftsakademie[8] judgments.

In the Working Party's 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")[9].
- The Working Party believe 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 targeted content and advertising.

As a consequence of acknowledging joint controllership, The Working Party also believe that:

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

The Working Party 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.

---

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

[8] C-210/16 *Wirtschaftsakademie*

[9] See Facebook's agreement with Page owners: https://www.facebook.com/legal/terms/page_controller_addendum

Necessity and proportionality of processing

We then assessed the processing and assured its necessity and proportionality. This has entailed assessing the legal basis for the processing, the protection of privacy principles and the rights and freedoms of users.

- 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. We believe 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 Inspectorate's interests in using the Facebook page when these interests are weighed against the processing of personal data in Facebook.

- Regarding privacy considerations; we refer to the risks identified in the systematic description of the data processing. At the same time, we have emphasized considerations of a more ethical nature, such as the Data Protection Authority's own values, reputation and capacity as a role model for privacy. We have reason to believe there will be several different and conflicting views on processing, both within and outside the organization. We do not believe, however, that the processing will have a deterring effect on the population.

The Working Party also highlight some relevant considerations from a privacy perspective, as well as suggestions for measures for improving privacy terms and conditions:

- However, 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. At the same time, we must be aware that Facebook can, at any time, amend these terms and conditions.
- The Working Party has identified some measures for improving privacy terms and conditions, and include transparency in the choice of communication platform, transparency in our assessments of the processing of personal data and of controllership for this processing (Page on Faceboook), as well as transparency of the practice of internal policies and moderations on the channel. We should also stay informed of any changes to Facebook's terms and conditions. In order to minimize data collection, no Facebook plug-ins or similar functionality would be implemented on our own website.

The Working Party have also made some assessments of processing in light of privacy principles and our impact on the data subjects' rights and freedoms:

The Data Protection Authority wishes all data processing taking place on a Facebook Page to be fair and respecting of the data subject's interests and reasonable expectations. Transparency about our internal policies on Page moderation and a dedicated contact person could contribute to this. Personal data collected by Facebook is used to make decisions about users and decisions that may affect users. It is uncertain how much personal data collected through the Data Protection Authority's Page on the platform would contribute to such decisions.

- The Working Party believe that the descriptions of the processing of personal data and considerations of accountability are characterized by a lack of transparency and clarification vis-à-vis Page owners and data subjects. 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.
- The Working Party believe 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 believe the Data Protection Authority's objectives, on their own, can be achieved by data minimisation; however, the platform does not permit that.
- The Working Party believe 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. The Working Partybelieve it to be 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.
- The Working Party believes that our options in terms of facilitating for and improving the rights and freedoms of the data subjects are minimal. A user would largely have to navigate the Facebook platform or contact Facebook in order to exercise their rights under the GDPR. 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.

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. In the Working Party's assessment, this has the following implications:

- We believe that Facebook's purposes are broad, vague and comprehensive. We believe it would be difficult for users to know what to expect from the subsequent processing.
- As a Page owner, we have no influence over what Facebook collects in terms of metadata, observational data and derived data when they interact with our Page.
- We believe it will be difficult for users to verify that their personal data is correct.
- We believe there are uncertainties associated with Facebook's actual storage periods.
- We believe there are several uncertainties associated with the way Facebook protects the rights and freedoms of data subjects. We question the real and full opportunity to exercise several of the data subject's rights under the GDPR against Facebook. The Data Protection Authority neither has access to nor influence over Facebook's subsequent processing of personal data, and consequently also neither access to nor influence over any processes that may put the data subject's rights and freedoms at risk.
- 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. Based on the assessments above, we find that the processing activities associated with a Facebook Page most likely do not comply with requirements of data protection by design and by default.

Assessment of risks to the data subjects' rights and freedoms

After considering the Authority's presence on a Facebook Page from the perspective of the Data Protection Authority being a data controller with a number of obligations pursuant to the GDPR, we flipped the perspective and considered the processing from the perspective of the data subject.

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 our findings from 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[10], as well as the Data Protection Authority's list of processing activities that always require a DPIA[11].

Assessment of co-determination, transparency and predictability

Our DPIA is based on the above criteria, and we assess *co-determination, transparency, predictability* in the processing, in accordance with the Data Protection Authority's own guide on data protection impact assessments. We do this to determine whether the processing can be performed in a manner that is acceptable and builds trust vis-à-vis the data subject.

Co-determination
We have assessed the degree of co-determination in light of the data subject's rights under the GDPR.

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

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, 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.

The data subject gives consent and is presented with the terms and conditions of the service when they create a profile on the platform. 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 Commissioner, or through the Norwegian supervisory authority.

As we have already pointed out above, we believe there are uncertainties associated with the true opportunity to exercise several of these rights, e.g. the completeness of access to one'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 will, however, have some degree of choice in the platform's user functionality and interface.

Generally speaking, the Working Party believes that data subjects may 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.

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

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

- 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.

Transparency.
Facebook describes the processing of personal data in its privacy policy, as well as in a wide range of other documents available on the platform. The Working Party nevertheless question whether Facebook provide users with sufficient information 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

The Working Party 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.

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. The Working Party believe Facebooks processing can be 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
- Possible 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 Working Party believe that the Data Protection Authority's processing in accordance with its own defined purposes will be perceived as limited in scope, clear, predictable and professional. We believe that most Facebook users will be used to communicating with Pages, and as such, this 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 subject 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:

- Collect the views of data subjects/representatives on processing, cf. Article 35 (9) of the GDPR.
- In addition to providing general information about processing, we can communicate our motivation for creating a Facebook Page and reflect on the choice of Facebook as a communication platform. This could help build trust in the data controller's processing, as well as show accountability and transparency.
- Consider making the risk assessment of Facebook available on request or consider proactively communicating this work, cf. ombudsman role.
- Refer to surveys, reports, research, etc. on Facebook and social media
- 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

In addition, we would like to point out the following:

- It would be up to the individual user to use Facebook and interact with our Page. Most people will already have a user account on the platform.
- Most of the information provided by the Data Protection Authority will already be publicly available and therefore not exclusively provided via Facebook. Communication in interaction with users, however, will be channel-specific.

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

The Working Party believes that this report has provided the Management Team with sufficient information on which to make a decision (note that this is an abridged version of the report). 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 processed by the Management Team more than once, but the risk to the data subject's rights and freedoms is still too high (and we are unable to mitigate it), the Management Team (Data Protection Authority) shall 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, in 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 may extend beyond those who 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, and should, insofar it is possible, ensure compliance with privacy laws. 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.

Office address:
Trelastgata 3, 0191 Oslo

Postal address:
PB 458 Sentrum
0105 Oslo

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

datatilsynet.no
personvernbloggen.no
twitter.com/datatilsynet