1. version, september 2018

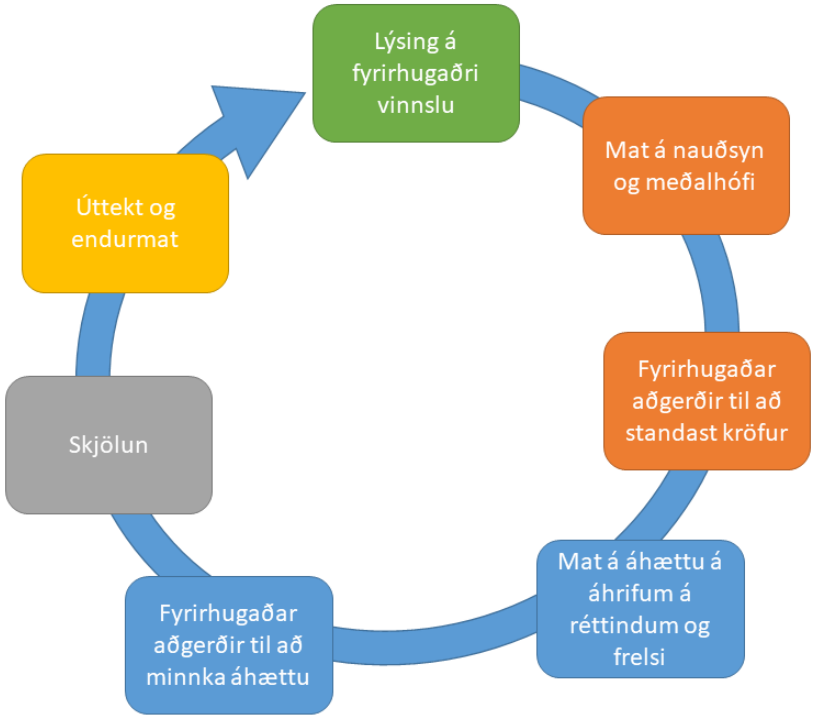
ASSESSMENT OF THE

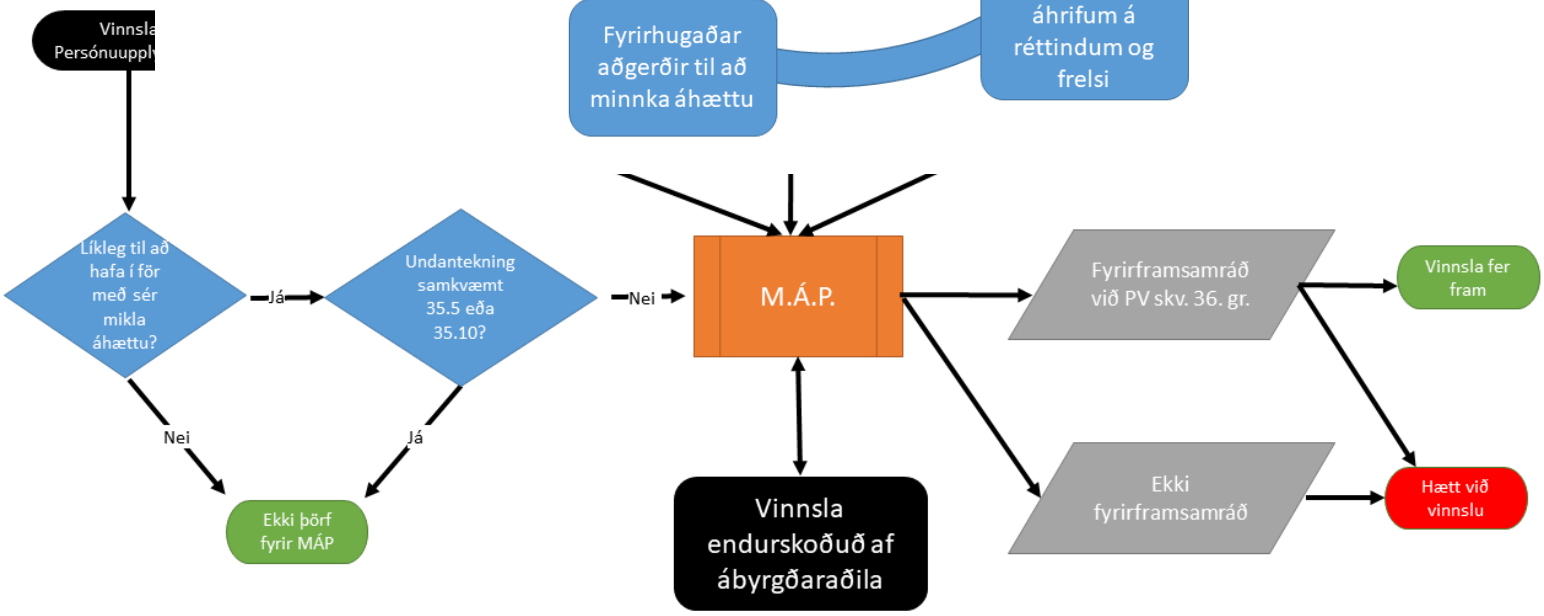
I

F

(

G





Privacy works to more detailed instructions for the implementation of MAP and will be the instructions
updated in accordance with it.

1. ver

2

Tabl

1.
What is MÁP?

Assessment of the impact on privacy is a systematic process that helps you to detect, identify and minimize persónuverndaráhættu of a project or system.
Usually is not possible to prevent all the risk, but it should be possible to minimize it and decide whether the risk is acceptable given the benefits.
MÁP is not just exercise. It to perform the assessment can detect possible problems before they become,
increased confidence and the confidence of their project covers and can in addition lead to savings if the project is
made simpler and less of the personal information is collected.
Make no assessment of the impact on the privacy where the circumstances demand it can in addition lead
to the levying of an administrative or other powers of the data Protection authority.

1.1 How is MÁP used?

MÁP can be performed for individual projects or a collection of related projects. It may even take advantage of
MÁP which was previously done for the corresponding task. A group of processors can also make common

MÁP for many similar or related projects.
For new projects is MÁP part of an integrated and default privacy. Best is to build
privacy into the project from the beginning when mestir options are to have effect on its potency.
However, do not forget to make MÁP if large-scale changes are made to the langtímavinnslu.

MÁP may not just be a form to be filled out and stored. It is a process that needs always to have in mind
from the beginning to the end of the project. For example, the need to reconsider the risks if you decide to collect additional
information, gildissviðið is expanded, öryggisgallar discovered or changes will be at the position of the public or legislators to specific risks.

1.2 More about MÁP

Persónuverndarreglugerðin makes a claim to MÁP is done under certain conditions before the processing
takes place.

1.2.1 What is the principle?

The principle is that MÁP should be carried out when a particular processing is likely to include significant
risks for the right of individuals to protect their privacy.

1.2.2 What does "significant risk"?

Risk in this context refers to the fact that the risk of significant harm to individuals. It needs both to take to how much the probability of damage and how much damage could become. ‘Significant risk’ can mean either that the greater the chances are that the damage will be or that the damage is greater, or whether
the two.

1.2.3 When needed to carry out the MÁP?

The regulation takes three examples of the processing that automatically requires the assessment of the impact on privacy.

- Processing which includes the extensive collection of personal information, the type of persónusniðs and use
for decision-making that has legal consequences for individuals
-

Extensive processing of sensitive information such as health, finances, genetic information
or sakaferil

Extensive monitoring of areas that are open to the public

Here's not about the completeness of the list to discuss. So can be the case of processing operations which involve a high
level of risk and are not certain in upptalningunni and needs therefore to perform MÁP.

The assessment of whether MÁP needs to take place may look to whether the processing involves any of
the following items:

1.
Evaluation of subjects, including.m.t. use persónusniðs, in particular to analyze or predict aspects concerning performance at work, financial situation, health, taste, interests, reliability or behaviour, location or mobility. An example of this could e.g. be when a credit institution conducts credit rating of a person by comparing the information together with the default, when líftæknifyrirtæki offers erfðaefnisrannsóknir directly to the consumer for the purpose of laying the
food on and set out the probability of specific risk factors, or a business that generates credentials for
marketing purposes on the basis of information about the behavior of the affected person into the website of the company.

2.
Automated decision making which has a legal effect to the purposes of the individual himself or touches
him in some way, to a large extent. Such decision-making may only be carried out with
certain conditions, e.g. when the individual has provided consent or agreed on it. Such processing
can lead to individuals being discriminated against and need therefore to go in MÁP.
1. version, October 2018

3.
Systematic monitoring.
Here covered, among other things, under the processing operations that take to structural and
extensive control of the area which is accessible to the public, e.g. the use of
eftirlitsmyndavéla or when the track is with the behavior and location of individuals on
a wireless network (e.g. wi-fi tracking).
This type of processing is dependent on the assessment of the impact due to the fact that in cases such as these can
personal information be collected in a situation where individuals do not realize
who is collecting the information, and how the information will be used or
processed. In addition, it may be impossible for individuals to avoid such processing, if
she goes out in public areas, or areas that are accessible to the public.
4.
Sensitive personal data or information of a personal nature
Here under the drop sensitive personal information, e.g. information about health status, ethnic origin,
sexual orientation and sex and personal data relating to convictions in criminal cases, and
punishable offense.
As an example we can mention here the preservation of the health of the medical records or the investigator
who has possession of personal information of individuals in criminal cases. At the same time there are
several categories of personal data of such a nature that the processing of their may incur
an increased risk. These data are considered to sensitive information as they relate to
the home and private life of the individuals involved, such as electronic
contact details, location information and financial information. Here may, however,
divided matter whether the information has been made public by the individual himself
or the other him irrelevant. Then you can at the same time fallen below data is taken to
your personal documents, dagbókafærslna, emails, etc.
5.
Extensive processing operations
Take should account for the following factors in assessing whether a vinnsluaðgerð is
extensive:

○

The number of registered individuals

○

The amount of the information to work with

○

Length or varanleiki of the processing

○

Geographic or regional scope of the processing

6.

Samkeyrsla

Here we can mention samkeyrslu that originates to trace in two or more processing operations, which are performed for different purposes and/or of different ábyrgðaraðilum in such a way, that the processing would take place from the realistic expectations of the individual.

7.
The personal data of vulnerable groups of persons
The processing of the personal data which is here in question is subject to MÁP because aðstöðumunar which potentially can be between the guarantor and the person that the processing relates to. This aðstöðumunur may mean that individuals are assessed not able to provide consent for the processing of personal data, the object of the operation going, or take advantage of their rights. To "vulnerable persons" in this sense may fall here under the children, workers, persons in need of special protection (e.g. mentally ill

persons, asylum seekers, the elderly, patients, etc.). What's relevant here is that the possible is to analyze the aðstöðumun that exist between the individual and the guarantor.
8.
Technological innovation or innovative methods of processing of personal data, e.g. the use of fingerprint readers are ready or andlitsgreiningartækni to regulate access to the housing, the use of the internet
of all things (e. internet of things), artificial intelligence, etc. note however that the technology needs to be new in the
tækniheiminum, not just for you.
9.
When is prevented for that individuals the enjoyment of their rights, or use a service or make contracts
Here may be mentioned processing operations which aim to allow, change or refuse the diversion of access to the service or contract, e.g., the type of credit ratings or the refusal of the insurance coverage.
As more of these criteria apply to processing that occurs, the more likely it is that the processing would result in a high risk for the rights and freedoms of individuals.
In most cases, companies and organizations assessed so that the processing that falls under the two aforementioned
criteria need MÁP. In some cases, can the result be that the processing of which takes one of the criteria, need assessment.
The following table shows how it is possible to use the criteria to assess whether a particular vinnsluaðgerð
need MÁP:
An example of processing operations
Criteria that may apply
Is a need
MÁP?
Processing
health
and
genetic information in the
medical facility.
-

Sensitive personal data or
information of a personal nature

-
Information relating to sensitive
individuals
-
Extensive processing operations
Yes
Use eftirlitsmyndavéla to
the fact that the patrols ökuhegðun on the
highways.
The data controller
intends to use the analysis system which
can amount to bifreiðaplötur and
differentiate them.
-
Organized monitoring
-
New methods or new solutions

Yes
Companies that viðhefur monitoring
with vinnuskilum, including. m.
shifts with the internet and
workspace.
-
Organized monitoring
-
Information relating to sensitive
individuals
Yes
The collection of social information
in order to equip credentials.
-
Food/fitness
-
Extensive processing operations

Yes
1. version, October 2018
7
Vinnsluaðgerð can fall under any of the above items, but could the result be that the processing is not likely to have a high degree of risk entailed. In such a situation, the need to justify and document the reason for the assessment of the impact should not be carried out. Then also need to specify the perspectives that persónuverndarfulltrúinn has acted, in effect, if he is present.

1.3 What does the "new technology"?

The regulation does not define what is a new technology. However refers to the technology which is a novelty in the tækniheiminum in the whole, not just new for you. The provisions of the regulation clearly stated that the application of new technologies can lead

- Samkeyrsla
- Sensitive information or information of a personal nature the Establishment carries out the assessment on the lánshæfni.
- Food/fitness
- Automated decision-making that has legal or other comparable, the effect.

Yes

Retention sensitive personal data which have been gerviauðkennd, their fragile individuals, due to the skjalavistunar, which are the subject of the research projects and klíniskra research.)

- Sensitive information
- Data which relating to the delicate individuals
-

Prevent the diversion of the enjoyment of rights, or running into contracts or use the services

Yes

The processing of personal data from the individual doctor, other professional healthcare professional or a lawyer about patients or clients. (91. gr. aðfararorðanna)

- Sensitive information or information of a personal nature

- Information about delicate individuals

No
Magazine that uses the mailing list to
send general (e. *daily*
digest?) to their subscribers.
-
Extensive vinnsluaðgerð
No
Electronic store displays on
the Internet advertising for
spare parts
in
fornbíla,
but
ads
appear
on
the basis of the
gerðrar
persónusniðs with reference to
their product that are viewed
or purchased on the website.

-
Food/fitness
No
1. version, October 2018
8
to MÁP must be carried out. When companies and organizations use new technologies to collect or work
with your personal data is likely to perform MÁP. Also can it mean when older technology is used in an innovative way. This is necessary due to the fact that the new technology can lead to innovative methods of data collection and use, which can entail a lot of risks for the rights and freedoms of registered persons. Of course, the risk posed by new technologies or new solutions, and/or methods of data collection or processing of personal data be unknown, but MÁP can assist companies and organizations to identify and deal with such risks.

1.4 What does the "systematic and extensive"?

The regulation does not define directly what is a systematic and extensive, but if compared with the older regulations may be defined progress as "systematic" if she is carried out according to the pre -
regularization program, is organized as part of the regular activities. "Extensive" implies that the processing will reach
to large regions, large amounts of personal data or of many individuals. Here may also need to take account of the size of the affected land, for example, processing that generally would not be considered extensive
in Europe be considered very extensive in the united kingdom where the case of a sparsely populated nation.

2.
There are exceptions from the requirement MÁP?

Impact assessment is not necessary in the following cases:

- If not, it is likely that a particular type of processing would result in a high risk for the rights and freedoms of individuals
- When the nature, scope, context and purpose of the processing are very similar to the processing that already
has gone through MÁP
- When vinnsluaðgerðirnar have been checked by the Privacy for the entry into force of new persónuverndarlaga.
- When prescribed by vinnsluaðgerðina in law and MÁP was carried out as part of the general áhrifamati we frumvarpsgerð. However, the legislature decided to MÁP shall be nevertheless carried out before the formal processing begins.
- If vinnsluaðgerð is on the list of those types of processing operations where there is required the evaluation of
the influence, which Privacy policy is allowed to give out. It is planned to publish such a list for the end of

year 2018.

3.

How to perform MÁP?

Assessment of the impact to perform before the processing begins. It is first and foremost the company itself or
the agency who is responsible to carry out the assessment, not the service provider or persónuverndarfulltrúinn.
However, it is possible to outsource the assessment but the responsibility lies with the ábyrgðaraðilanum. Then you need to seek the advice
provided persónuverndarfulltrúa, if he exists, when the assessment is carried out and it is necessary to
document the evaluation them the advice that he gives.
If the processing is in whole or in part prepared by the service providers or processors, carries him to assist
the controller to ensure that the obligations according to the legislation are met and provide the necessary
information.

It may be necessary to seek the views of persons who work on the information or their representatives.
You can obtain their opinion, e.g. by directing questions to the representatives of the staff or send a survey
on the customers. If the controller decides to not need to seek the opinion of the individuals which the processing
purposes, then he may need to document it, e.g. if it is believed compromising the business plans of the company to
inform about the proposed processing. Then it can also simply be out of moderation, inefficient and too
costly.

When a specific business entity lay especially to MÁP carried out, they should be involved in the assessment and submit proposals. Then it may be appropriate to seek the views of external experts who
belong to different professions (lawyers, upplýsingatæknifræðinga, öryggisfræðinga, siðfræðinga, félagsfræðinga etc.)
Öryggisstjórar and persónuverndarfulltrúar can also proposed to MÁP is carried out on a particular vinnsluaðgerð. Then should these parties also to assist and supervise the preparation of the evaluation, including.on m. in order to
assess its quality and whether the level of risk that still exists is acceptable.
Responsible parties can be dedicated to a different methodology for the implementation of the evaluation, but the criteria are
they the same.

The regulation specifies certain lágmarksþætti that the assessment needs to be stored:

- A systematic description of the fyrirhugðum vinnsluaðgerðum and purpose with the operation going
- The assessment of whether vinnsluaðgerðirnar are necessary and modest
- The assessment of the risks for the rights and freedoms of registered persons
- The measures planned to take against such risks and arrangement to demonstrate the compliance with this regulation

The following diagram shows using a graphical means it as a general process that constantly needs to be
established with the implementation of the MÁP:
1. version, October 2018
10
Take due consideration of whether the relevant responsible parties or converters follow
the statutes hátternisreglum when the effect of processing operations téðra the controller or processors are
evaluated. This can be useful for the controller to demonstrate that he has taken
adequate measures, assuming that the hátternisreglurnar are appropriate given the vinnsluaðgerðina.
Then it should also take into account vottana, seal, mark, and binding fyrirtækjareglna to the assessment of whether
the processing operations as responsible parties or converters are responsible, are in accordance with the provisions
of the regulation.
The requirements that the regulation allows for the evaluation of the effect of providing, in a way, a broad and general framework
for the design and implementation of the evaluation. The regulation provides ábyrgðaraðilum flexibility to
decide how they will exactly behave the structure and the type of assessment on the impact on privacy.
Regardless of what type or type of assessment will be chosen, then there will be assessment of the impact to be
the actual assessment of the risks posed by vinnsluaðgerð, so the responsible parties can practiced these
steps in order to cater to the risk.
It is the role of the controller to select the methodology used is the implementation of the evaluation of the effect,
but to a minimum to compliance with the criteria of Privacy has laid out:

3.1 Athugunarlisti the result of the implementation of the assessment of the impact on privacy

1.
A systematic description of the proposed vinnsluaðgerðum, which includes:
○
The nature, scope, context and purpose of the processing;
○
About which personal data is involved, who are the recipients and varðveislutími;
○
Description of the proposed vinnsluaðgerðum;
1. version, October 2018
11
○
A description of the upplýsingaeignum (hardware, software, networks, people, paper) as
used for the processing.
○
Information about whether compliance with the statutes hátternisreglum
2.

Are vinnsluaðgerðirnar necessary and modest relative to the purpose?:
○
Certain have been measures that aim to demonstrate compliance with
the regulation:
▯
Reasoned description of the measures that contribute to the need and meðalhófi
of the solution and apply to the following items:
▯
Is the purpose clearly specified and legitimate?
▯
Is to present sufficient authority for the operation going (consent,
contract, legal obligation, public interest, legitimate interests
, etc.)? See more of 6.-9. gr. pvrg.
▯
Are the information that the work with which adequate, relevant and
limited to what is necessary?
▯
Has been taken the attitude to it at any time delete no information (in
case the government needs to take into account the surrender to the archives).
▯
Reasoned description of the measures that contribute to the rights of the sign and take the
minimum to the following items:
▯
How is education to the diversion arranged? See 12., 13. and 14. gr. pvrg.
▯
How is the insured the right of individuals to access to the
personal data and the right to transfer your data, if it applies? See
15. and 20. gr. pvrg.
▯
How is the right to correction and the right to be forgotten?
See 16., 17. and 19. gr. pvrg.
▯
How is insured andmælaréttur and the right to restriction of processing
See 18., 19., and 21. gr. pvrg.
▯
The description of the relationship with processors, is he present. See 28. gr. pvrg.
▯
It is planned to transfer information out of the EEA area? What
protective measures to take, such as the recipient's within the safe
third of the state, created to confirm the binding fyrirtækjareglur or make a
standard contract terms? See section V of the pvrg.
▯
Fyrirframsamráð with Privacy
3.
Risks and threats for the rights and freedoms of registered persons defined
○
The origin, nature, particularity and severity of the risk are evaluated from the point of view of the
sign

(such as a wrongful access, unwanted changes and destruction of information).
▯
The origin of the risk is defined. See 90. the preamble to the pvrg.
▯
The possible impact on the rights and freedoms of the sign are defined in cases that can lead to ólögmæts access, change and deletion of information.
▯
Threats that can lead to ólögmæts access, alteration or deletion are defined.
1. version, October 2018

▯
Evaluated are the probability and severity. See 90. the preamble to the pvrg.
4.
What measures are proposed to reduce the risks.
○
Example: Encryption, gerviauðkenni, access control, etc.
5.
Consultation with the parties concerned:
○
Seek the advice provided persónuverndarfulltrúar and documented his advice and why not go to his advice, if applicable.
○
Seek the opinion of those subjects that the processing relates to or their representatives on the intended processing, when applicable.
6.
Conclusion MÁP
○
If the risks are still too high relative to the defined criteria, there are three ways available:
▯
Stop with the proposed processing of personal data.
▯
Resort to additional measures, e.g. the stronger the encryption, to reduce the amount of personal information collected, the access of the employees is limited to specific employees, etc.
▯
Search fyrirframsamráðs with Privacy, if the controller can not be derived from the risk at an acceptable way.

3.2 Is standard on the implementation of the MÁP?

No, but it is planned that such a standard will be given out on the road ISO:
ISO/IEC 29134 (project),

Information technology – Security techniques – Privacy impact assessment – Guidelines .

4. Further reading

▯

Vurdering av personvernkonsekvenser (DPIA), Datatilsynet

Standard Data Protection Model, V. 1.0 – Trial version, 201631, Datenschutzzentrum.

Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española
de protección de datos (AGPD).

Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL).

Conducting privacy impact assessments code of practice, the Information Commissioner's Office (ICO).

i

At the first meeting of the european persónuverndarráðsins on 25. may 2018 was declared full support with the instructions 29. gr. the working group had given out because of the new persónuverndarreglugerðarinnar.