Factsheet

on the data protection impact assessment (DPIA)
in accordance with Articles 22 and 23 FADP

August 2023

Sources

- Federal Gazette 2017 6941 Dispatch on the Federal Act on the total revision of the Federal Act on Data Protection and the amendment of other enactments on data protection (Dispatch)

- Lobsiger Adrian ‘Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation', Schweizerische Juristenzeitung SJZ 6/119

Table of contents

1 Object and purposes of the DPIA

From 1 September 2023, in accordance with Articles 22 and 23 of the revised Data Protection Act (FADP), a **data protection impact assessment (DPIA)** must be carried out if processing is likely to result in a high risk to a data subject's personality or fundamental rights (Art. 22 para. 1 FADP).

As a working instrument of modern data protection law, the DPIA aims to safeguard the rights of data subjects in the social reality of digitalisation. As Article 23 paragraph 1 FADP states, the object of the DPIA is primarily **planned processing of personal data**, whereby legislators were focusing mainly on large-scale digital transformation projects. This does not necessarily have to involve **new processing of personal data**. The object of a DPIA can also be developments and extensions of **existing processing of personal data**.

The purpose of the DPIA is to ensure the **early identification of significant project risks,** focusing on the **probability of their occurrence** and, when they are qualified as 'high', to the **significance** of their effects.

The purpose of the DPIA is not limited to the **foreseeability and assessment of 'high' project risks**. Rather, the practical benefit of this working tool lies in **documenting** the source and analysis of systemic and security risks in a comprehensible manner and using suitable **measures** to reduce them to a level acceptable from a data protection perspective.

2 What the DPIA is seeking to protect

In terms of Article 22 paragraph 1 and Article 23 paragraph 1 FADP, 'high risks' in terms of these provisions must relate to the data subjects' personality or fundamental rights. The law thus defines the protection of personality rights as the core concern of data protection, with **privacy and informational self-determination** being what is **primarily protected** by means of a DPIA, including an individual's autonomy, dignity and identity. With regard to protecting informational self-determination, the dispatch to the FADP also states that a 'high risk' is to be assumed if the specific characteristics of the planned processing of personal data indicate that the freedom of the data subject to do as they wish with their data will or may be restricted to a high degree.

If personal data are processed unlawfully, this may result in physical and financial **consequential damage** which may affect legal interests and fundamental rights other than the primary objects of protection of data protection law, such as the right to life or physical integrity or to property. This additional damage can be occasioned not only the data subjects affected by the processing, but also the data controllers as a result of the causal chain.

To illustrate this, consider the following fictitious example: a humanitarian association operates a digital project, processing statistics on politically persecuted migrants. In the course of an initial risk assessment, the association comes to the following conclusions:

- *The planned processing is associated with a potentially high risk to the privacy and informational self-determination of the migrants concerned. Conclusions could be drawn from the data subjects' private contact data that are incompatible with the purpose of the processing and could end up in the wrong hands (primary risk for the data subjects).*
- *The primary risk may be accompanied by the consequential risk to the data subjects that they could be unlawfully persecuted or even murdered (consequential risk for the data subjects).*

- *This consequential risk to the data subjects could give rise to an associated risk for the data controllers, who could suffer reputational damage and be required to compensate the data subjects financially (consequential risks for the data controllers).*

With regard to the distinction made in the example between **primary and consequential risks**, the FDPIC recommends that data controllers responsible for evaluating the 'high risk' identify:

- in a first step, the risks to the primary objects of protection, i.e. the privacy and informational self-determination of the data subjects, and
- in a second step, the consequential risks to their other legally protected rights and fundamental rights.

Where consequential risks **affect the data controllers themselves**, this is hardly relevant from a supervisory perspective, because Articles 1 and 22 paragraph 1 of the FADP are not aimed at protecting data controllers, but at safeguarding the personality and fundamental rights of data subjects. It could be different if the consequential risks potentially increase the damage and risks borne by the data subjects. For example, if insolvency means a controller is no longer able to pay for technical infrastructure required to protect the personal data that it processes.

3 Characterisation of 'high risk'

Apart from the provisions on the DPIA in Articles 22 and 23, the FADP mentions personal data processing with a 'high risk' in the provisions:

- on 'high-risk profiling' under Article 5 letter g;
- on the obligation to appoint a representative in Switzerland under Article 14 paragraph 1 letter d;
- on notification of data security breaches under Article 24;
- on the processing of personal data to verify the creditworthiness of the data subject under Article 31 paragraph 2 letter c. number 1.

Due to its need for interpretation, the rather vague legal term 'high risk' means that data controllers and the federal data protection supervisory authority may see an unreasonable level of risk in an excessively wide range of situations. Since the legislator has also avoided any precise definition, the term will only become clearer as it is applied in practice and becomes the subject of case law.

3.1 General definition of high risk (Article 22 para. 2 first section FADP)

It should not be overlooked that the legislator provides interpretation guidelines in Article 22 paragraph 2. According to this provision, a 'high risk' may derive from

- the nature,
- the extent,
- the circumstances and
- the purpose

of the processing, which indicates a broad discretion to apply the law. The **nature** of processing that can typically pose a high risk incudes profiling if it allows an **assessment of essential aspects of a** data subject's **personality** within the meaning of Article 5 letter g. Other forms of automated processing, such as automated individual decision-making within the meaning of Article 21 FADP, can also lead to a high risk. With regard to the **circumstances**

of processing, the fact of the data subject being a subordinate of the data controller may, for example, come into play.

3.2 Absolute criteria according to Article 22 paragraph 2 letters a and b FADP

Article 22 paragraph 2 letters a and b FADP provide a non-exhaustive list of absolute criteria, the fulfilment of which is deemed by law to constitute a 'high risk':

- the extensive processing of sensitive data, and
- the systematic and extensive surveillance of public areas.

4 Preliminary risk assessment pursuant to Article 22 paragraphs. 1 and 2 FADP

If it becomes apparent that a planned processing operation could be associated with high risks, the data controller must carry out a (summary) preliminary assessment of the risks associated with the operation. The criteria mentioned in section 3, which apply to the DSFA itself, are the guiding principles for the preliminary risk assessment.

The preliminary assessment must be carried out as early as possible, i.e. already during **project planning**, even if the details of data processing have not yet been defined. It may therefore be advisable to provide for variants.

It is advisable to prepare a processing directory and a systematic description of the processing operations and purposes of the planned processing operations, including business models and other intentions and interests of those responsible for the project. When expanding and developing **existing applications**, a **comparison** must always be made between the previous and the planned processing operation.

The result of the preliminary assessment and the underlying assessments must be **documented**. If the result is inconclusive, it is advisable to carry out a DPIA.

The flow chart in Annex 1 provides more information about the procedure and additional criteria for the preliminary assessment.

The Federal Office of Justice will provide risk assessment aids for federal bodies that process personal data, which can also be used by private data controllers.

Obligation to carry out the DPIA (Art. 22 para. 3 FADP)

If the preliminary assessment has shown that a planned processing operation could carry a high risk, a DPIA must be carried out. The provisions of Article 7 FADP (privacy by design and by default) require that a DPIA, like the preliminary assessment, must be carried out as early as possible. As many details are usually still unavailable, it may be advisable, as in the preliminary assessment, to devise variants that are adapted and reduced in the course of the process.

If the FDPIC learns of a planned processing operation and is of the opinion that the controller must carry out a preliminary assessment and then a DPIA before carrying out the processing, the FDPIC can intervene as the statutory supervisor to stop the planned processing if the controller refuses to carry out the assessment (see point 8 below).

4.1 Content and structure of the DPIA

Article 22 paragraph 3 FADP requires that a DPIA must include:

- a **description of the planned processing**,
- an **evaluation of the risks** and
- a description of the **measures**

for the protection of the personality and fundamental rights of the data subjects, i.e. the primary and secondary objects of protection (see Sec. 2 above). A template for structuring a DPIA is provided in Annex 2.

4.2 Description of the planned processing

First of all, the descriptions and comparisons drawn up in the course of the preliminary assessment must be updated in accordance with Section 4 and then examined in greater depth in the course of the actual DPIA. For further details, please refer to Annex 2.

4.3 Description and assessment of the potentially high initial risks

Sections 1-3 provide a description of the potentially high primary and secondary risks that a planned personal data processing operation could carry and their evaluation according to probability of occurrence and severity.

If personal data are transferred abroad, the transfer itself is subject to an evaluation, which must be integrated into the DPIA. This is especially important when exporting to countries that do not have an adequate level of data protection, which could lead to potentially high risks. Data controllers are unable to **demonstrably influence** these risks because they lack practical or legal means of influence, with the result that the residual risk indicated in the DPIA must remain high. This may be the case, for example, if there is a threat of potential violations of personality rights and fundamental rights due to the scope of what foreign authorities can do in practice under foreign law. Often the data controller will be unable to influence this risk with any legal certainty, whether by contractual arrangements or by recourse to legal action. This means that the controller cannot reliably assess the probability of occurrence and potential severity of the violation even after planning and identifying appropriate measures in the DPIA.

The transparent disclosure of such risk situations in the DPIA includes, if applicable, the disclosure of the fact that they cannot be reliably assessed. Depending on the effectiveness of the technical, legal and organisational measures taken, these transparency requirements may become relevant in particular if personal data are to be outsourced to operators of data centres belonging to groups based in countries whose legal system does not provide a level of data protection comparable to that under Swiss law.

4.4 Planned measures to reduce the potentially high initial risks

The measures required in Article 22 paragraph 3 FADP to protect the personality and fundamental rights of the data subjects aim to reduce the anticipated high initial risks arising from the intended processing to an appropriately reduced level, so that the risk can then be classified as less high or lower than high. The measures considered may involve a balancing of the interests of the data subject against those of the controller. The result of this balancing of interests must also be mentioned and justified in the DPIA.

Annex 2 provides further details on the description of the planned protection measures.

4.5 Remaining end risks

Article 23 paragraph 1 FADP explicitly assumes that certain forms of data processing - depending on the circumstances - may still exceed the threshold of 'high risk' even after taking the protective measures that appear appropriate and reasonable to the data controllers. The FADP therefore does not require data controllers or the FDPIC to reduce potentially high processing risks to any particular level specified by law, or even to ensure that they are eliminated.

However, data controllers must identify all the end risks and their causes in the DPIA in an understandable complete manner and must satisfy themselves that the end risks of a planned processing operation that are still assessed as 'high' are acceptable when considering the requirements of the data protection legislation as a whole. Only if this prerequisite is met can the processing in question be reasonable for the data subjects in terms of its planned scope and detail and thus justifiable overall.

Annex 2 provides further information on the description and evaluation of end risks.

5 Procedure after completion of the DPIA

Depending on the assessment of the identified end risk, the following procedures must be followed:

5.1 No high end risk

a) Even if the remaining end risk is less than 'high', the controller must check whether the planned processing is compatible with all the requirements of data protection legislation. Only once this basic condition has been met may the processing be carried out.

b) The controller does not have to submit the DPIA to the FDPIC.

   If the controller voluntarily submits the DPIA to the FDPIC, the latter is not required to act on it and take a substantive position. However, the FDPIC may, within the scope of its advisory activities, comment in certain cases on residual risks that are no longer high. The FDPIC must charge a fee for this advice (see Art. 59 para. 1 let. e FADP).

5.2 High end risk

a) If data processing is to be carried out despite a high residual risk, which is permissible in principle, the residual risk must be indicated clearly to the data subjects. This also includes disclosing risks that can neither be influenced nor reliably assessed. With regard to giving consent that justifies high end risks being taken, private data controllers should note that consent to high end risks may only be given if it is informed consent, i.e. the person giving consent must be aware of the residual risks indicated in the DPIA.

b) According to Article 23 paragraph 1 FADP, the DPIA must be submitted to the FDPIC for an opinion. The opinion is subject to a fee (Art. 59 let. c FADP).

   According to Article 23 paragraph 4, private data controllers are not required to consult the FDPIC if they have consulted their data protection officer. In this case, however, the DPIA may be submitted to the FDPIC on a voluntary basis. If the FDPIC agrees, its assessment is subject to a fee pursuant to Article 59 paragraph 1 letter c FADP.

6 Procedure if high-risk processing leads to a breach of data security

If there are sufficient indications that circumstances could arise in which existing or modified processing becomes associated with additional risks that are generally assessed as high, the data controller must prepare a new DPIA or update the already existing DPIA. This need may be triggered by expert reports, complaints from data subjects, media reports, cyberattacks that have been averted or carried out without damaging intent, or any other breach of data security. If the new or updated DPIA shows a high residual risk, the data controller must submit it to the FDPIC for an opinion, including a comparison of the previous applications with the applications being expanded.

If, in the course of processing personal data, there is a breach of data security involving high risks for the data subjects that is subject to notification to the FDPIC in accordance with Article 24 FADP, the data controller must take the necessary measures in good time to restore the lawful position and to inform the data subjects of any violations or potential violations of their personality or fundamental rights that have occurred. If it becomes apparent that the risks of processing are likely to remain high if it continues, the FDPIC may request the data controller to carry out a DPIA.

7 Opinion of the FDPIC following submission of a DPIA

The FDPIC checks whether the DPIA submitted shows and explains all the high end risks in a clear and comprehensible manner. Furthermore, it examines whether the planned processing, taking account of the identified risks, is compatible with the requirements of the data protection legislation as a whole, in that it is acceptable to the data subjects in terms of its planned scope and detail, and thus justifiable overall.

The FDPIC must notify the data controller of any objections and proposed amendments within the two-month period specified in Article 23 paragraph 2 FADP. The FDPIC's opinion is subject to a fee (Art. 59 FADP). The opinion may relate to the planned data processing or also to the structuring of the DPIA, e.g. if the controller does not adequately assess and identify the imminent risks.

The opinion of the FDPIC should be regarded as a recommendation and therefore does not constitute approval or authorisation for the planned processing to go ahead.

8 Supervisory measures taken by the FDPIC

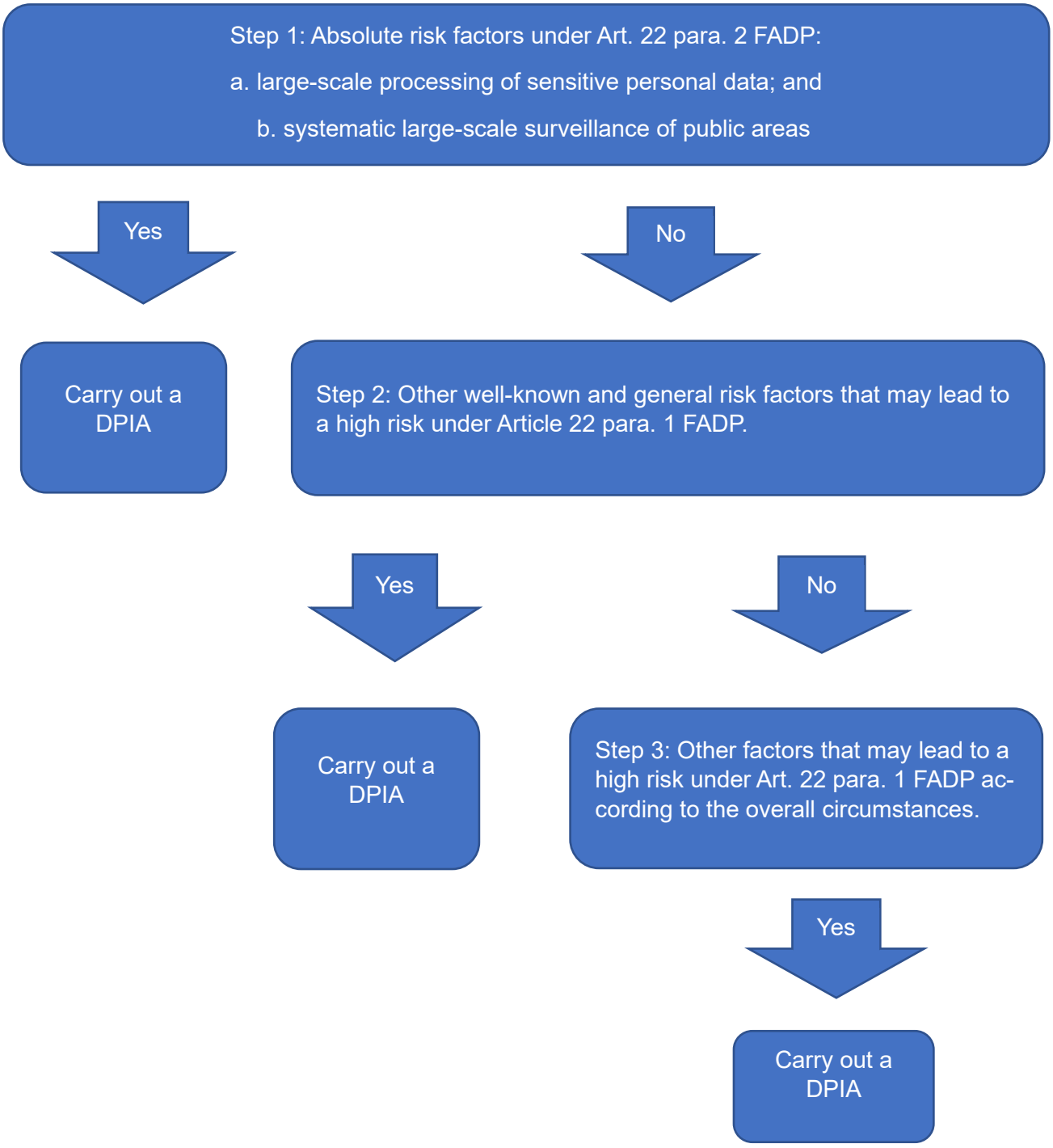
If a data controller refuses to comply with significant objections or suggestions made by the FDPIC, the latter may open an investigation and in due course formally order the changes it has proposed, up to and including a ban on processing the data. In doing so, the FDPIC must respects the discretionary powers that the data controllers, as experts in their professional field and or business sector, have when assessing processing risks.

Formal action by the FDPIC is particularly advisable where it is unreasonable to accept a risk, especially in view of the probability of problems occurring and severity of the breaches of personality rights, and the planned processing is therefore not permitted under data protection law. For example, this would be the case if processing with a high residual risk would violate data protection principles, such as the requirement of proportionality in Article 6 FADP or the technical security requirements in Article 8 FADP. The question of whether and to what extent data controllers may require data subjects to accept high residual risks that cannot be reliably assessed according to the DPIA, cannot be answered by referring to the provisions of the DPIA, but only by considering the data protection legislation as a whole.

Annex 1

Flowchart for the preliminary assessment of whether a DPIA must be carried out

The following flow chart can be used for the preliminary assessment pursuant to Article 22 paragraph 1 FADP:



Explanation of the flow chart

The following steps can be used to check whether a DPIA needs to be carried out.

Step 1:

If at least one of the absolute risk factors is present, a DPIA must be carried out.

If there is no specific risk factor, proceed to Step 2

Step 2:

It must be established whether there are one or more risks likely to arise in the processing of the data (including those in the following non-exhaustive list).

- Is there high-risk of profiling?
- Is an automated individual decision being made?
- Are new technologies, including artificial intelligence, being used?
- Is the personal data obtained secretly (without the knowledge of the data subject)?
- Does the data processing concern a large amount of data or a large number of persons?
- Is the data processing being carried out for a long time or does it concern a large geographical area?
- Are data sets linked or compared with each other?
- Will the personal data be disclosed to third parties?
- Does the processing of personal data lead to the monitoring of the data subjects?
- Are the data subjects prevented from exercising a right, using a service or performing a contract?

If any well-known risk factors apply, a DPIA should be carried out in case of doubt.

If there is no well-known risk factor, proceed to Step 3

Step 3:

It must be examined whether, taking into account all the circumstances, the data processing may lead to a high risk to the personality or fundamental rights of the data subjects.

If so, a DPIA should be carried out.

If not, a DPIA is not necessary.

Annex 2

Part 1: Template for structuring a DPIA

The following list can be used as a template for structuring a DSFA:

1. Data controller

- Data controller
- Data Protection Commissioner
- Other internal bodies involved
- Processor
- Joint controllers

2. Context of the data processing operation

- Description of the actual situation
- Description of the target situation
- For existing applications that are being expanded: comparisons of the actual and target situations and reference to already existing DPIAs

3. Data processing

- Legal basis (public) / justification (private)
- Purpose of the data processing
- Data subjects
  - Category (employees, customers, patients, etc.)
  - Involvement (opt-in/opt-out; automated processing; transparency)
- Type of data:
  - Text, image, sound, etc.
- Data categories
  - Personal data, sensitive data, etc.
- Scope of data processing/quantity of data
  - Number of data subjects
  - Data volume per data subject
- Data quality
  - Sources/method of collection
- Geographical scope
- Duration/detail of processing
- Deletion deadlines
- Technical aspects
  - Technologies used
  - Data handling processes
  - Encryption

    - IT systems and interfaces
    - Data storage
    - Access permissions
- Compliance with data protection principles
    - Legality
    - Good faith
    - Earmarking
    - Proportionality
    - Transparency
    - Data correctness
    - Data security
    - Data security/technical risks: Possibly ISDS concept, etc.
- Implementation of privacy by design/by default

4. Potentially high risks before measures (initial risks)

- Nature of the risks
    - Systemic risks
    - Legal risks
    - Security risks
    - Are these primary risks to the privacy and informational self-determination of the data subjects?
    - Are these secondary risks to other legal interests or fundamental rights of the data subjects

- Analysis and assessment of the potentially high initial risks
    - Data subjects (persons whose data are processed or data controllers)
    - Scope
    - Probability of occurrence

5. Measures to reduce the potentially high initial risks

- Legal measures
    - Contracts, SCC, etc.
- Organisational measures
    - Selection, instruction, supervision of staff
    - Awareness raising, training
- Security measures

6. Risks after measures (end risks)

- Impact of the measures taken on the potentially high initial risks
- Risks can be influenced by measures taken by the data controller
- Risks cannot be influenced by measures taken by the data controller (e.g. access by foreign authorities)
- Proportionality of the measures/weighing of interests

7. Result

- High end risk
- High end risk acceptable or unacceptable under data protection law?
- High end risk eliminated or no longer high

8. Consultation FDPIC

- High end risk despite measures
- Exception: consultation with internal data protection officers