Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner
FDPIC

Data Protection

Guidelines on reporting data security breaches and informing data subjects in accordance with Article 24 FADP

From 6 February 2025, last updated on 23 April 2025 (Version 1.2)

Versions

Version 1.0	06.02.2025	Publication
Version 1.1	26.02.2025	Clarification of wording in sections 1.2 and 1.7
Version 1.2	23.04.2025	New section 1.2 Reporting Person and clarification of wording in (new) section 1.4 voluntary reports

Inhalt

In its very first article, the Data Protection Act (DPA) states that its aim is to protect the personality and fundamental rights of natural persons whose data is processed. Article 24 FADP governs the obligations of data controllers and the rights of data subjects in the event of a breach of data security when personal data are processed. Under Article 5 letter h FADP, a data security breach is to be assumed if personal data are accidentally or unlawfully lost, deleted, destroyed or modified, or if the data are disclosed or made accessible to unauthorised persons.

Data security breaches that lead to serious breaches of business and manufacturing secrecy, official secrecy or professional secrecy but do not affect personal data therefore do not fall within the scope of Article 24 FADP. The same applies to data that relate exclusively to people who are dead and do not allow any conclusions to be drawn about people who are still alive that would violate their personality rights, as Article 31 paragraph 1 of the Swiss Civil Code provides that personality ends on death.

The FDPIC guidelines deal with the legal notification requirements for data security breaches to the FDPIC, in particular the notion of a 'likely high risk' as defined in art. 24 para. 1 FADP. They also define the requirements for informing the data subjects in the event of a data security breach in accordance with art. 24 para. 4 FADP.

1 Reporting data security breaches to the FCPIC

1.1 Content of the report

The report must contain a description of the circumstances of the breach and the controller's assessment of its implications, and include in particular details of the type, time, duration and extent of the breach and its already known and anticipated effects on the data subjects. Article 15 paragraph 1 of the Data Protection Ordinance (DPA) lists the information that may enable the FDPIC to take the steps required to help the persons affected by the data breach, e.g., by ordering that they be informed of the incident (see Section 2 below).

1.2 Reporting Person

Notifications to the FDPIC (as well as informing the data subjects) are the responsibility of the controller. The data processor, for his or her part, is obliged to inform the controller of any breach of data security. This duty to inform is not subject to a risk assessment as in Article 24 paragraph 1 FADP; the data processor must inform the controller of any breach of data security, regardless of whether it is likely to result in a high risk to the privacy or fundamental rights of the data subject.

1.3 Duty to report

Under Article 24 paragraph 1 FADP, the controller must report a data security breach to the FDPIC as soon as possible after becoming aware of it if the breach is likely to result in a high risk to the personality or fundamental rights of the data subject. If it becomes apparent to the controller based on the risk analysis carried out during or immediately after the data security breach that a high risk likely exists and it cannot be determined with certainty, or at least not within a short period of time (on the question of risk, see Section 1.5 below), the controller must notify the FDPIC of the data security breach. For example, in the case of ransomware attacks, depending on the circumstances, an initial analysis will have to assume a "likely high risk". The person responsible must report "as quickly as possible" according to the law and therefore cannot wait in such cases for the results of more lengthy investigations that can unequivocally confirm or exclude the likely high risk.

The mandatory report must contain all the information listed in Article 15 paragraph 1 DPO, although paragraph 2 (see Section 1.4 below) permits details to be reported later if they are not immediately available.

If the controller fails to file this report, the FDPIC, on becoming aware of the breach, may order the controller to provide the required information (Art. 51 para. 3 let. f FADP).

On receipt of the report, the FDPIC quickly examines whether the immediate and follow-up measures taken or planned by the controller to protect the data subjects and mitigate the consequences (see Art. 15 para. 1 let. f DPO) appear suitable and sufficient, and appropriate in terms of time. If necessary, the FDPIC will first ask the controller to clarify the circumstances described and assessments made and to modify or supplement the measures taken or planned. If need be, the FDPIC will also contact the controller to ensure that the incident is documented, e.g., by securing log data. The FDPIC will also check whether data subjects have been made adequately aware of the incident and its consequences (see Art. 15 paras 3 and 4 DPO). If the controller fails to comply with the FDPIC's requests, the latter may open a formal investigation under Art. 49 FADP and enforce the requests with measures under Art. 51 FADP.

If the public interest so requires, the FDPIC may also inform the public of its findings and orders on the basis of Article 57 paragraph 2 FADP.

1.4 Voluntary reports

Practice has shown that controllers may also wish to report data security breaches to the FDPIC where no high risk has been identified. The FDPIC also accepts such voluntary reports. Those voluntary reports have proven to be useful for all parties concerned and also expedient from the point of view of public interest, especially in cases where the risk analysis indicates a low risk because of the data involved, but where media interest may arise, for example due to the large number of persons affected (see Section 1.5 below).

After a summary review of the report, the FDPIC decides whether to order any measures to inform the data subjects or the public or whether to take such measures itself.

1.5 Making a report

Reports must be submitted to the FDPIC as quickly as possible and formulated in such a way that they describe the circumstances underlying the data security breach and its effects as fully as possible. If it is not possible for the controller to provide all the information at the same time, the controller has to provide the missing information as soon as possible (see Article 15 paragraph 2 DPO).

The FDPIC provides a reporting portal (link) for mandatory reports, which guarantees the secure transmission of data to the FDPIC. The interactive form also ensures that the report contains all the information required in Article 15 paragraph 1 DPO, thus guaranteeing that the reporting obligation is correctly fulfilled. In addition, the reporting portal issues confirmation of the time of reporting and allows follow-up reports, which can be filed to supplement the report at any time.

Voluntary reports, on the other hand, are made outside the reporting portal and, as explained above, do not automatically trigger any action by the FDPIC.

1.6 High risk in terms of Article 24 paragraph 1 FADP

Under Article 24 paragraph 1 FADP, the controller must notify the FDPIC of a data security breach as soon as possible after becoming aware of it if it is likely to result in a high risk to the personality or fundamental rights of the data subject.

The FADP uses the expressions 'high risk' and 'likely to lead to a high risk' in a number of provisions. When interpreting 'high risk', due consideration must be given to the different purposes of these provisions.

When assessing high risk in accordance with Article 24 paragraph 1 FADP, data controllers should firstly clarify the extent to which the data security breach that has occurred has already harmed the personality or fundamental rights of natural persons. Secondly, the criterion of 'likelihood' mentioned in the provision requires controllers to include in their assessment the consequences of the data breach for the persons potentially affected, which can neither be conclusively measured nor can be predicted with certainty when assessing their obligation to report.

The likely high risk mentioned in Article 24 paragraph 1 FADP must be identified without taking into account measures that the controller only plans, announces or initiates after the data security breach. The FDPIC's previous practice when assessing the risk, however, was to take account of immediate measures that controllers were able to take even before submitting the report in good time where these

measures demonstrably excluded or minimised the anticipated effects of any personal data breach. This was the case, for example, where a controller quickly regained control of personal data that had been made temporarily inaccessible by taking immediate measures and was able to establish with sufficient certainty within hours on the basis of logs or other evidence that the data had not been processed improperly. However, in situations of doubt where a high risk cannot be sufficiently excluded, controllers must not wait before fulfilling their reporting obligation. For example, a controller has to file a report before deciding whether to pay cybercriminals a ransom for stolen data and long before trying to work out whether or how data recovered after paying a ransom have been processed by the criminals.

The criteria for assessing the likelihood of a high risk resulting from the data breach are:

1.6.1 The severity of the consequences:

The first step is to assess the severity of the harm to the personality or fundamental rights of the natural persons affected by the data breach that has already occurred or is anticipated. The level of harm to those most severely affected is what counts. The following criteria can be taken into account when assessing the severity of the harm:

- Need to protect the personal data concerned: The type of personal data affected by the data breach is a key aspect of the assessment. The more sensitive these data are, the higher the risk that data subjects' personality or fundamental rights will be violated. If particularly sensitive personal data in accordance with Article 5 letter c FADP are affected, e.g. health data, biometric data or data on social assistance measures, a high risk must be assumed in many cases. However, a breach involving data that do not fall into this category, such as (copies of) identity documents or credit card details, can also pose a high risk. Depending on the context in which the personal data affected by a data security breach are processed, a 'likely high risk' must therefore also be assumed for personal data that are not especially sensitive. This is the case, for example, where contact or address data affected by a data security breach have been processed by an authorised party in the course of criminal proceedings or when providing social assistance, i.e. in cases in which sensitive data as defined in Article 5 letter c FADP are regularly processed. If the personal data concerned were already publicly accessible before the data breach, the risk is normally not categorised as high.
- The nature and circumstances of the breach and the identity and motives of the unauthorised third parties: When carrying out the risk assessment, it can make a difference whether the data security breach has been caused by human error, criminal intent or a technical fault. The risk assessment can vary depending on the cause. However, if personal data are lost and then become accessible to the general public, e.g. through publication on the darknet, this tends to lead to the risk being assessed as high, regardless of whether the data got there as a result of a technical fault or criminal activity. On the other hand, where personal data on the controller's server are deleted simply with the intention of causing damage, this may indicate a lower risk. However, a controller's subjective but unsubstantiated trust in the good intentions of unknown data recipients is not enough to rule out an objectively high risk.
- Effort required to identify persons: Another criterion that applies in the risk assessment is the amount of work and money that is needed in order to process information that has been unlawfully obtained and possibly made available to the general public, e.g. on the darknet, in order to be able to draw any conclusions about identifiable persons. The easier it is to draw conclusions about a specific person from the unlawfully obtained data, the higher the risk is for that person. For example, if all that is lost is a customer number but no further data is available that can be used to identify the person from the customer number, the risk is lower than if e-mail addresses (Vorname.Name@XXXX.com) that clearly identify a person are involved. If personal data affected by a data security breach have been effectively encrypted by the controller, they remain unreadable to anyone who does not have the key. Encrypted data are therefore considered anonymous under data protection law for all third parties who are not authorised to access them, with the result that the loss of encrypted data does not need to be reported under Article 24 paragraph 1 FADP. In contrast, data affected by a data security breach that have only been pseudonymised are considered personal data, which may lead to a reporting obligation under this provision.

- Quantity and processing time: When determining the level of harm, the amount of information affected by a data breach and time needed to process it in relation to a specific individual can be a decisive factor.
- Intangible and financial harm: Serious consequences for the individual affected can be assumed if a data security breach enables abuses such as identity theft or credit card fraud, which result in harm such as reputational damage, discrimination or financial loss, which in turn cause personal distress such as worry or anxiety to victims.
- Vulnerable persons: For example, if a data security breach affects the data of minors or people with disabilities, this can also indicate that serious consequences may ensue.
- Total number of persons and volume of data affected by the data breach: A high number of data subjects or large volumes of personal data do not in themselves mean that the risk must be high. However, in the case of data breaches involving a large number of data subjects, there may be a public and private interest in informing the persons affected. In practice, it is not uncommon for data controllers to voluntarily report such data security breaches to the FDPIC (see Section 1.3).

1.6.2 Likelihood of anticipated consequences:

After a data security breach has occurred and been recognised by the controller, the controller must assess the likelihood that the effects of the data security breach, which at this stage can still not be conclusively assessed or have not yet occurred, will actually cause the anticipated harm to those most affected. This likelihood will have to be estimated as higher for a hospital affected by a data security breach, for example, which processes a large amount of sensitive personal data in addition to administrative and scientific data, than for a food distributor, for example. Accordingly, a hospital, if the subject of a breach, is not permitted to delay reporting a data security breach to the FDPIC while it establishes whether not only factual information but also patient data have been affected. When assessing the likelihood of occurrence, measures that the controllers only planned, announced or initiated after the data security breach occurred must be disregarded. This means that the controllers may not wait for measures to be implemented and evaluated before informing the FDPIC of a data security breach that must be reported because of the high potential for damage.

1.7 Reporting data security breaches to the FDPIC and freedom of information

The activities of the FDPIC as the federal supervisory authority for data protection are subject to the Federal Act on Freedom of Information in the Administration (Freedom of Information Act, FoIA; SR 152.3). Reports from controllers, in whatever form they are made, as well as any communications between the FDPIC and controllers or their processors are in principle to be regarded as official documents in terms of the FoIA. Official documents produced by the FDPIC in the exercise of its statutory duties in handling data security breaches are therefore in principle accessible to the public under the FoIA. This applies in particular to all reports of data security breaches, regardless of whether they were made under the obligation set out in Article 24 paragraph 1 FADP or voluntarily. When dealing with access requests under the FoIA, the FDPIC examines whether and to what extent any access may be restricted or deferred, based on the exceptions provided for in Article 7 ff. FoIA. As part of the procedure, the FDPIC must hear any third parties concerned in advance. It decides on access by issuing an opinion or, if so requested, by means of a ruling. The mediation procedure pursuant to Article 13 f FoIA does not apply (see the judgment of the Federal Administrative Court A-4781/2019 of 17 June 2020, E.3).

1.8 Reporting obligation and sanctions

Where a controller should have informed the FDPIC of a data security breach in accordance with Article 24 paragraph 1 FADP, but failed to do so, the FDPIC, on becoming aware of the breach by some other means, may order the controller to comply with the reporting obligation (Article 51 paragraph 3 letter f FADP). The FDPIC may also impose further administrative measures in connection with a data security breach, e.g. if the requirements of Article 8 FADP have not been met.

A failure to comply with the reporting obligation as such, in whole or in part, is not a criminal offence under the FADP. However, a data security breach may be a criminal offence if, for example, the controller has not complied with the minimum data security requirements (Article 61 letter c FADP). Article 24 paragraph 6 FADP stipulates that mandatory reports may not be used in criminal proceedings without

the consent of the person subject to the reporting obligation. This also applies to voluntary notifications (see also Basler Kommentar Datenschutzgesetz, 4th edition [BSK] Article 24 N 98 with reference to MÉTILLE/MEYER, in Meier/Métille (eds.), Commentaire romand, Loi fédérale sur la protection des données, Basel 2023, Article 24 N 35).

2 Informing those affected by the data breach

A distinction must be made between the controller's duty to report under Article 24 paragraph 1 FADP and its duty to inform the persons affected by the data security breach. Under Article 24 paragraph 4 FADP, the controller must inform the data subjects about the data security breach if this is necessary to protect these persons or if the FDPIC requests it.

The obligation to notify the data subjects pursuant to paragraph 4 is to be interpreted independently of paragraph 1 and the concept of high risk used there (see MATHYS/THOMANN, in Vasella/Blechta (eds.), BSK Article 24 N 63).

If the controller can credibly demonstrate that the data subjects are already sufficiently aware of a data breach and its consequences without requiring additional information and that they know what measures they can or must take to protect themselves, the duty to inform can be deemed to have been fulfilled.

2.1 Obligation to provide information because data subjects require to take action to protect themselves

It must be assumed that data subjects require the protection referred to in Article 24 paragraph 4 FADP if they can or must take action themselves to minimise or avert harm from a data security breach. For example, if they have to change access data or passwords (see Dispatch on the revised FADP, BBl 2017 6941 ff., 7065). However, there may also be a need for data subjects to take action in other cases, e.g. if credit cards have to be blocked, or account statements or messages and enquiries, i.e. phishing e-mails, have to be critically examined (see MATHYS/THOMANN, BSK, Article 24 N 67).

The 'likely high risk' pursuant to paragraph 1 of Article 24 FADP, which triggers the controller's obligation to notify the FDPIC, is not legally essential in order to establish an obligation to inform the data subjects pursuant to paragraph 4 of the same provision. This duty to inform applies where a controller can reasonably argue on the basis of its insider knowledge that there is no objectively high risk, but those potentially affected by a data security breach are unsure of the situation and expect the worst. Conversely, the existence of an anticipated high risk in terms of Article 24 paragraph 1 FADP will generally also indicate an obligation to provide information in accordance with paragraph 4 of this provision.

2.2 Obligation to provide information based on a request from the FDPIC

Under Article 24 paragraph 4 FADP, the FDPIC may require the controller to inform the data subjects. The FDPIC may issue this request irrespective of whether the controller has previously reported the breach voluntarily or made a mandatory report pursuant to Article 24 paragraph 1 FADP or indeed if the controller has made no report at all.

The FDPIC will require the controller to inform the parties involved if, in its opinion, the need to protect those affected by the data security breach requires this. However, it can also demand it because it believes that, due to the large number of data subjects affected or the media coverage, there is a public interest in the controllers providing the large number of data subjects and thus indirectly also the general public with more detailed information on the consequences of a data security breach in an appropriate manner. An interest of this kind may arise in particular if consequences that could give rise to fears and speculation among the general public can be prevented or significantly minimised. In such cases, controllers often decide in practice to make voluntary reports to the FDPIC, which the FDPIC welcomes (see Section 1.3; Right to report above).

In addition, the FDPIC has the authority to inform the public of its findings in these cases, based on Article 57 paragraph 2 FADP, as they are cases of general interest. However, it is normally simpler for the data controller to inform the data subjects itself.

2.3 Provision of information

Pursuant to Article 15 paragraph 3 DPO, the information given to data subjects must be provided in 'simple and comprehensible language' and must contain at least the following details: the form of the breach, i.e. what happened, the consequences of the breach, including the risks to the data subjects, and the measures that have been taken or are planned to remedy the breach and to minimise the consequences. The name and contact details of a contact person must also be provided.

There are no requirements as to the form in which the information is provided, and the controller must choose the appropriate method.

Normally, the data subjects are informed directly and individually. In exceptional cases, the information may be provided in a public announcement in accordance with Article 24 paragraph 5 letter c FADP, provided the individual data subjects are informed in a comparable manner. The duty to inform is not overridden by the public announcement, but only modified (see CÉLIAN HIRSCH, Le devoir d'informer lors d'une violation de la sécurité des données. Avec un regard particulier sur les données bancaires, Genève 2023, p. 315).

2.4 Duty to inform and sanctions

If the controller is required to inform the data subjects of a data security breach in accordance with Article 24 paragraph 4 FADP because of their need to take action or because it has been requested to do so by the FDPIC, the FDPIC may order the controller to comply with the reporting obligation in the event of any failure or refusal to provide information (Article 51 paragraph 3 letter f FADP). The FDPIC may also take further administrative measures in connection with a data security breach, for example if the requirements of Article 8 FADP have not been met.