



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner
FDPIC

Version 1.0

FDPIC technical recommendations for logging in accordance with Article 4 DPO

of 15 September 2023

Table of contents

- 1. Introduction and aim of the document 3
 - 1.1. Article 4 DPO 3
 - 1.2. Article 3 paragraph 3 DPO 3
 - 1.3. Purpose of logging 4
- 2. Logging..... 4
 - 2.1. The three aspects of logging 4
 - 2.1.1. Recording..... 4
 - 2.1.2. Storage 4
 - 2.1.3. Analysis..... 4
 - 2.2. Concept..... 5
- 3. Technical recommendations 5
 - 3.1. General technical recommendations for logging..... 5
 - 3.2. Storage and storage volume 6
 - 3.3. Logging for existing applications..... 7
- 4. Specific questions on implementation / FAQs10

1. Introduction and aim of the document

With Article 4 DPO¹ coming into force on 01.09.2023², a private controller and its private processor must as a minimum log the storage, alteration, reading, disclosure, deletion and destruction of data during the automated processing of personal data.

These recommendations are intended to provide a summary of what is involved in this form of logging and what needs to be done to comply with Article 4 DPO in technical terms. The various system owners must decide how the requirements are actually implemented thereafter; this is not part of these recommendations. In addition to those of the FADP, other requirements, such as those relating to information security, may also be relevant. The aim is to achieve the most efficient and effective logging possible by avoiding duplication.

1.1. Article 4 DPO

The wording of the Article 4 DPO, which has the heading 'Logging', is as follows:

¹ If a large volume of sensitive personal data is processed by automated means or if high-risk profiling is carried out and if preventive measures are unable to guarantee data protection, the private controller and its private processor must as a minimum log the storage, alteration, reading, disclosure, deletion and destruction of the data. A log file must in particular be kept if otherwise it would not be possible to establish whether the data has been processed for the purposes for which it was collected or disclosed.

² The responsible federal body and its processor shall in the case of automated processing of personal data log as a minimum the storage, alteration, reading, disclosure, deletion and destruction of the data.

³ In the case of personal data that are generally accessible to the public, logs shall be kept as a minimum of the storage, alteration, deletion and destruction of the data.

⁴ The log file must provide information about the identity of the person that carried out the processing, the form, date and time of processing, and, if applicable, the identity of the recipient of the data.

⁵ The log files must be retained for at least one year and kept separate from the system in which the personal data are processed. They may only be made accessible to the bodies and persons that are required to review the application of the data protection regulations or to safeguard or restore the confidentiality, integrity, availability and traceability of the data, and may only be used for this purpose.

1.2. Article 3 paragraph 3 DPO

Logging is intended to ensure the traceability of the processing and, in particular, access to personal data. This is set out in Article 3 paragraph 3 DPA, which describes the objective of logging:

³ In order to guarantee traceability, the controller and the processor must take appropriate measures to ensure that:

- a. it can be verified what personal data were entered or altered in the automated data processing system at what time and by which person (entry control);
- b. it can be verified to whom personal data are disclosed with the aid of data transmission devices (disclosure control);
- c. breaches of data security are recognised rapidly (recognition) and measures are taken to mitigate or eliminate the consequences (elimination).

¹ [Ordinance of 31 August 2022 on Data Protection \(Data Protection Ordinance, DPA, SR 235.11\) \(admin.ch\)](#)

Traceability also includes reading the data, which is done by recording accesses in order to detect a breach of data access control in accordance with paragraph 3 letter c.

1.3. Purpose of logging

The purpose of logging is to make the processing of personal data verifiable at a later time, so that it can be determined in retrospect whether data have been accessed or whether the data have been deleted, destroyed or altered. Logging also serves to ensure conformity of purpose and adequate data security, as well as providing information on whether personal data have been processed in accordance with the stated purpose of processing. In addition, the logs can also be used to detect and investigate breaches of data security. However, logging must not be evaluated for the purpose of monitoring the behaviour of users who process personal data.

2. Logging

Logging under data protection law means the systematic recording of information about the processing of personal data. The purpose of logging is to ensure transparency and accountability and, in the event of data protection breaches or incidents, to be able to trace who accessed what personal data, when, and what was changed.

2.1. The three aspects of logging

The three aspects of logging are the recording, storing and analysing of log data.

A private controller and its private processor must as a minimum keep a record of the storage, alteration, reading, disclosure, deletion and destruction of data. A log must be kept particularly if it cannot otherwise be determined retrospectively whether the data were processed for the purposes for which they were obtained or disclosed.

The process of 'reading' should be understood as accessing data without 'altering' them; it is therefore sufficient if access to personal data and the alteration of these data are logged. This means that any 'reading' has been logged. Reference should be made here to the restriction in Article 4 paragraph 3 DPO for personal data that is generally accessible to the public. Here, as a minimum the storage, alteration, deletion and destruction of the data must be logged, i.e. 'reading' does not need to be logged.

2.1.1. Recording

Log data must be recorded to ensure that there is a record of all operations involving personal data. This means that any form of access (by persons or machines) to personal data must be logged, including the identity of the person who carried out the processing, the type, date and time of processing and, if applicable, the identity of the recipient of the data.

2.1.2. Storage

Log data must be stored securely. Log data must be stored separately from data processing systems to ensure that the data remain available even if the primary system is compromised (e.g. by ransomware). Access may only be granted to authorised persons who are responsible for verifying compliance with the data protection provisions or for maintaining or restoring the confidentiality, integrity, availability and traceability of the data.

2.1.3. Analysis

It must be possible to analyse the log data when necessary to detect possible data protection breaches and to ensure that any access to personal data is lawful. This requires powerful analytical tools that are able to process large amounts of log data and identify patterns or

anomalies that indicate possible breaches. The log data must only be accessible to the bodies and persons who are responsible for checking the application of the data protection provisions or for maintaining or restoring the confidentiality, integrity, availability and traceability of the data, and may only be used for this purpose (Art.4 para. 5 DPO).

2.2. Concept

A logging concept must be drawn up and should include a comprehensive and systematic description of the logging policy and procedures. Essentially, the following points should be considered:

- a) Objectives of logging: The concept should define clear goals to be achieved by logging, e.g. monitoring the processing of personal data, security monitoring, troubleshooting.
- b) Protocol guidelines: The concept should set out clear guidelines for logging, including what events are logged, what data are collected, what storage time is envisaged and who is allowed to access the log data.
- c) Logging tools: The concept should describe the tools that are used for logging, e.g. log generation agents, log management tools, event logging frameworks or security information and event management (SIEM) systems.
- d) Alerts concept: The concept should describe which events can generate alerts, how alerts are reacted to, who must be notified and what measures must be taken when problems are detected.
- e) Responsibilities and roles: The concept should define clear responsibilities and roles for logging management, e.g. who is responsible for monitoring logging, who assigns the rights to do so and who updates the logging policies. Furthermore, it must be explained who is responsible for the analysis and reporting.
- f) Training: The concept should describe how employees involved in logging can acquire the necessary knowledge and skills to work effectively and securely.
- g) Review: The concept should provide for regular reviews of logging policies and procedures to ensure that they are effective and in line with current requirements.

A comprehensive concept serving as a basis for examining the appropriateness and proportionality of the logging policy, together with compliance with any order for statutory access to logging data, is crucial.

3. Technical recommendations

3.1. General technical recommendations for logging

There are a number of technical recommendations for logging in relation to information security or data protection. The most important aspects are listed below:

- a) Use of standardised logging formats: The use of standardised logging formats such as Syslog or Common Event Format (CEF) help to ensure a uniform logging of events.
- b) Ingestion and interpretation of protocols: Logs should not only be stored, but also ingested and interpreted (parsing and indexing). This is the basis for monitoring, detecting and issuing alerts on anomalies. In doing so, all information elements should be extracted during ingestion using pattern extraction and supplemented with information from existing protocols where appropriate (correlation). Unused

information fields should be omitted from this process in order, not least, to save storage space.

- c) Regular review of the log data: Log data should be checked regularly to ensure that they are complete, that security guidelines are being followed and to ensure that they have not been tampered with.
- d) Anomaly detection mechanisms: Anomaly detection mechanisms should be applied to the log data (e.g. detecting access from unusual geolocations) in order to detect suspicious activities. To do this, it is first necessary to define normal behaviour in order then to be able to detect changes.
- e) Use of security measures for log data: It is important to subject log data to appropriate access controls to ensure that the data are protected from unauthorised access.
- f) Timestamp: The log data must be time-stamped to record the exact time of an event in the system. An accurate timestamp is important for understanding the chronological relationship between different events in the system.
- g) Time synchronisation: To ensure accurate time stamps, it is important that all systems on the network have reliable and accurate time synchronisation. Synchronising the clocks of all systems via a common NTP server ensures that the log data is accurate and consistent.
- h) Data enrichment: Data enrichment adds additional information to the log data to enable a better understanding of events. For example, geo-information, user context or system configuration data can be added. This allows log data to be better analysed and potential security threats to be detected more quickly. With data enrichment, it is important only to add information which is relevant and necessary for actually achieving the goal (of logging). When linking to other data or profiling with the aid of enrichment, the data protection officer, if available, must be involved. If a processor is commissioned to carry out data enrichment, it must also be ensured that a legally valid contract exists between the client and the processor that fulfils the requirements under the DPO.
- i) Alerts: The logging analysis applications used should be capable of informing the controllers immediately if anomalies or known safety-relevant events occur.

By implementing these technical recommendations, private controllers can achieve comprehensive logging that enables effective monitoring and analysis of and response to security-related events.

3.2. Storage and storage volume

One challenge in processing log data is the required storage volume. For the analysis tools, log data should remain directly accessible for as long as is needed to detect and respond to data breaches or security incidents. This can vary depending on the type and size of the organisation, but typically covers a period of a few days to several weeks. During this period, the data can be actively used to detect and respond to suspicious activity.

After the log data are no longer needed directly for analysis but, for example, are still required for checking compliance with data protection regulations, they can be moved to a longer-term storage system. This allows the data to be copied and compressed into cheaper storage space. This, of course, does not mean that the data can be kept for a longer retention period than provided for in the relevant legislation. The following recommendations apply:

- a) Use of suitable storage media: For long-term storage of log data, suitable storage media should be used that offer long life and reliability.
- b) Storage period: It is important to define a clear retention period for log data to ensure that they are not kept for an unnecessarily long time. It goes without saying that the legal requirements for the retention period must be complied with. The storage period for log data in connection with the processing of personal data is a minimum of one year.
- c) Calculate storage volume: To calculate the required storage volume for log data, various factors must be taken into account, such as the amount of log data generated, the number of systems in the network and the duration of storage. It is important to provide sufficient storage capacity to prevent the logging process from being interrupted. When planning the storage volumes and estimating the relevant costs, it can be assumed from the recommendation that the data normally remain in the index for 1-2 weeks and then have to be kept in the long-term storage system for at least one year.

In summary, the long-term storage of log data is part of the data security strategy and it is important that the log data are stored separately from data processing systems (in accordance with Art. 4 DPO) to ensure their integrity and availability. An additional backup copy of the log data on another system is usually not necessary as long as a robust storage solution is available and the data are regularly checked for integrity and completeness. However, it must be decided on a case-by-case basis whether a backup of the log data is necessary.

3.3. Logging for existing applications

For new applications, it is relatively easy to log all activities involving personal data from the beginning. With existing, older applications, however, it is not always possible to adapt the application itself. However, there are various approaches to solving these difficulties.

Carrying out logging depends on many factors, such as the programming language, the runtime environment and the development methods used for the application. Our recommendations are therefore generic in nature, but can assist in planning for specific applications.

Step 1: Know the logging requirements for the application

Find out how long the logs should be indexed and remain in the long-term memory. The (legally required) retention period affects the calculation of storage and data volumes (last step 5).

Step 2: Know the processing operations to be logged

Not all activities in an application constitute the processing of personal data and need to be logged. A list of the relevant activities helps to focus on the adjustments that are needed. Logging is ultimately about recording the activities that are important in terms of the DPO and not about logging as many activities as possible.

In applications where personal data are processed but it is not obvious in advance exactly what activities take place (e.g. a documentation system), all activities must be logged.

To strengthen the information security of the application, it may also be desirable to log security-critical events.

Step 3: Know the information flows that trigger processing activities

There are different types of applications:

- In most, there is communication (i.e. a flow of information) between the presentation level (the front end) and the administrative logic (the back end) when processing personal data. The information often flows through several networks and security systems (shown as an example in Figure 1), which see at least part of the activities and can therefore be useful in logging with regard to information security.

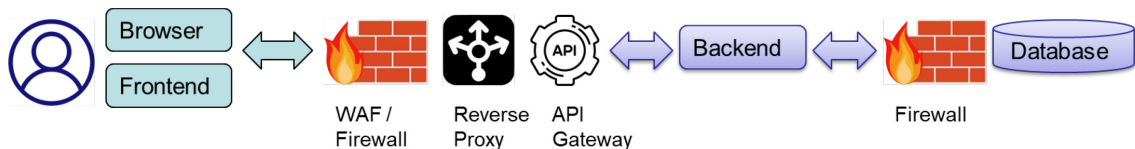


Figure 1 - Possible information flow in the application

- For applications where processing takes place only at the user's end and there is no communication with server-side backends or databases, the initial download to the user's system should be logged as 'access'. In this case, changes can usually only be recorded by extending the application itself, which would only make sense in exceptional cases.
- Another use case is applications in which the processing is carried out autonomously by a process in the backend (e.g. the automated linking of various personal data to profiles, the automated expansion of personal data such as user IDs with the corresponding names, etc.). Here, too, an extension of the application itself will often be necessary.

Step 4: Decide where logging can and should be included

Once it is known where logs need to be generated for activities and what the information flows look like, it is possible to work out how logging can most easily be retrofitted. The NCSC recommends the following procedure:

1. Applications often already support the logging of activities, but this feature is disabled and must be switched on. First of all, check whether this is the case. If an existing logging function covers all activities and contains enough information (i.e. the identity of the person receiving or processing the personal data and the activity of processing), this is the simplest approach.
2. It may be that enough information about the activity is already visible in the network systems (e.g. the user ID based on the IP address and the activity in relation to the backend). If this is the case, the firewall or *web application firewall* (WAF) protocols may already be sufficient to meet the requirements.
3. Web servers or HTTP reverse proxies often see the decrypted requests. These systems also support the logging of activities and can selectively capture communication requests and forward them to a log analysis system.
4. In more modern applications, API gateways are also used to accept all requests from the user to the backend or between backends (in the case of automated processing) in order to forward them to the correct target backend. These see the content of the requests and logging can be retrofitted there without changing the applications themselves.
5. Reading or modifying personal data is mostly done via database systems. These almost always also support the logging of the corresponding requests.
6. If none of the previous recommendations offer a solution, the application must be extended. In order not to modify the application itself, it is sometimes possible to write

a 'wrapper': this is a new application that receives all requests, logs them and then passes them on to the actual application, but otherwise makes no changes.

Step 5: Calculate the storage volumes and decide on the analysis systems.

With the help of the decisions from the previous steps, the storage volumes can now be calculated (see Chapter 3.3) and a decision can be made on the ingestion and monitoring of the logs with the service provider for the target system.

4. Specific questions on implementation / FAQs

The following questions from the field were brought to the attention of the NCSC. Further questions will be added to the list as may be required:

1) *Do all the recommendations set out in the document have to be implemented?*

The logging recommendations are general in nature. In order to ensure the cyber security of the systems - and a certain traceability after incidents - logging is a necessity.

Art. 4 DPO does not specify whether and which analysis tool should be used and we assume that many data processing systems are capable of performing the logging that is additionally required 'out of the box'.

The Ordinance only requires log data to be copied and stored separately. For data protection purposes only, unlike cyber security, these do not need to be held or 'analysed' in online storage.

2) *What does 'generally accessible to the public' mean? How can this be reliably determined?*

Access is possible without authentication, e.g. on a web server.

The term 'generally accessible to the public' refers to information that is widely accessible, such as an address search via a website. According to the exception in Article 4 paragraph 3 DPO, only the storage, alteration, deletion and destruction of such personal data must be logged. The aim of this provision is to make it clear that the ingestion and disclosure of such personal data does not have to be logged.

3) *Which level-of-assurance is permitted for determining identity (under Art. 4, paragraph 4 DPO) for logging (Google ID, Facebook or 2-FA)?*

Logging relates to the identity(ies) of the person(s) involved in the data processing and is in this sense independent of the LoA

4) *What happens if current systems cannot and will not meet these requirements?*

Virtually every known system can log in some form. Otherwise, there are third-party applications that can do this. If there is no third-party application in a particular case, then a suitable solution would have to be developed or the recommendations under point 3.3 would have to be taken into account in order to comply with the requirements.

5) *Is a backup of the log data also separate storage under Article 4 paragraph 5 DPO?*

A backup of the log data would already satisfy the requirement for separate storage under Article 2 paragraph 5 DPO. The purpose of separate storage, apart from the additional security against a possible attacker, is also to prevent these data from being encrypted in the event of a ransomware incident.

6) *Does the execution of automatic scripts also have to be logged?*

If these scripts can store, modify, read, disclose, delete or destroy the personal data - then yes. The aim of logging is to ensure the traceability of data processing procedures. This can be done, for example, by recording the start time, end time, script version, and identity of the processor.

7) *What about NAS, SAN and other unstructured data storage? Example: Open a Word document from the directory O:\Abteilung_A\Daten\Register\xy.docx. Would such accesses have to be logged?*

Article 4 paragraph 1 DPO is to be understood in relation to Article 3 paragraph 3 letter a DPO in such a way that the obligation to log only relates to personal data in automated data processing systems. In the scenario described in the question, accesses do not have to be logged.

8) *Do all logs have to be stored in the same place?*

Not necessarily and it may also not be realistic - for logging it is important that logs are available and can be merged in a meaningful way. Firewall logs, for example, can be stored in a different location from the Active Directory logs, as long as changes and accesses to the personal data remain reconstructible. For information security, it is also important that the logs have been merged in such a way that anomalies can be detected.

9) *Can external Log Management as a Service solutions be used?*

If possible, the legal service and the data protection officer for the company should be consulted if this is being considered, as the risks in relation to personal data tend to increase rather than decrease. We advise against it.
An exception would be if the processing itself was already operated as SaaS - assuming that the above-mentioned persons have already been consulted.

10) *For each document, personal data (of the staff involved) also accrue in the metadata, particularly regarding creation, changes and comments. We assume that these personal data do not have to be logged in accordance with Article 4 DPO.*

Yes, that is correct. The purpose of logging is to protect the personal data processed (i.e. contained in a document). However, the fact that new personal data are generated again because these personal data have been processed (because person X created the document, changed it, etc.) does not give rise to a new reason for logging. The personal data generated to ensure the traceability of the data processing are not themselves the subject of the logging.