The General Data Protection Regulation

Guidelines on the retention periods of personal data by payment service providers

Date of first adoption: 06/06/2025

Table of contents

Introduction

1. Those guidelines are primarily addressed to payment service providers ('PSPs' or 'controllers') within the meaning of the amended Law of 10 November 2009 on payment services[1] ('the 2009 Law').[2]

2. Payment service providers collect and process a significant amount of personal data, at the time of entering into a relationship, throughout the duration of the relationship, and even well after the end of the relationship with the user of the service ('the user' or 'data subject'). Furthermore, technological innovations have significantly increased the ability of payment service providers to collect, store, combine and analyse a wide range of data about their users.

3. Personal data that may be processed by PSPs may include information on the personal situation of the data subject (age, nationality, marital status, etc.), his or her economic and financial situation, payment data (such as the amount of the transaction, the date and time of payment, the identity of the beneficiary of a transaction, IBAN or personalised security data), the data subject's anti-fraud score, contextual or behavioural data (consumption preferences and habits, geolocation, characteristics of the terminal used for an online purchase, time spent prospecting, etc.).

4. However, although they do not enjoy a special status under the General Data Protection Regulation (EU) 2016/679 ('GDPR'), many of those data are to be regarded as 'sensitive' data (in the common sense of the term) in so far as their infringement could have serious implications for the daily life of the data subject.[3]

5. Given the scale of such processing, the CNPD would like to recall some of the key principles of Article 5 GDPR as regards the processing of payment service users' data. A PSP may process the personal data of a data subject only if the intended processing is **lawful;** i.e. necessary for the performance of the contract with the user, necessary for compliance with a legal obligation to which the PSP is subject, necessary for the purposes of the legitimate interests pursued by the PSP or, in rarer cases, on one of the other legal bases for the processing of data mentioned in Article 6 GDPR. In accordance with the principle of **transparency,** data subjects must retain control over the data concerning them. This presupposes that they are clearly informed of the use that will be made of their data as soon as they are collected and throughout the life cycle of the processing. In addition, users' personal data may be processed only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (principle of **purpose limitation).** The data must also be adequate, relevant and limited to what is necessary for the purposes for which they are processed (data **minimisation**

[1] https://www.cssf.lu/fr/Document/loi-du-10-novembre-2009/

[2] While the principles set out in these guidelines may also apply to other professionals in the financial sector, the purpose of this guidance is not to set out the specificities applicable to other professionals.

[3] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and how to determine whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679, WP248 rev.01 – endorsed by the EDPB (p.11); Guidelines 6/2020 on the interaction between the Second Payment Services Directive and the GDPR, Version 2.0, Adopted on 15 December 2020 (§69)

principle). They must also be accurate and, if necessary, kept up to date (principle of **accuracy).**

6. Finally, according to Article 5.1(e) GDPR, personal data must be 'kept *in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed*...' (principle of **data retention limitation).** These guidelines will not address in detail the issue of data necessary for the performance of contracts that are retained for the duration of the contractual relationship but rather all aspects relating to retention periods once that relationship with the data subject has ended. Indeed, PSPs generally retain the personal data of their users in order to comply with certain legal obligations or to protect themselves from certain legal actions during the periods of legal prescriptions.

7. Without claiming to be exhaustive, the purpose of these guidelines is to provide stakeholders with information on the retention periods and arrangements for the personal data they process in the context of a highly regulated sector. The protection of personal data is increasingly anchored in the various European regulations (also those applicable specifically to the financial sector) and the CNPD would like to inform as much as possible the controllers concerned on the application of some of these provisions in relation to the requirements of the GDPR on retention periods for personal data. With the presence of numerous payment service providers acting as controllers based in Luxembourg[4] and in accordance with the recommendations of the European Data Protection Board ('EDPB') and the European legislator, the CNPD intends to adopt a holistic approach to the regulatory framework applicable to financial sector actors, in cooperation with the other competent authorities in Luxembourg.[5][6]

[4] In May 2025, there are 117 credit institutions, 17 payment institutions and 12 electronic money institutions in Luxembourg (source: https://www.cssf.lu/wp-content/uploads/newsletter292.pdf)

[5] See *EDPB Strategy 2024-2027:* 'The *EDPB will work to strengthen cooperation with other regulatory authorities, with a view to integrating the right to data protection into the overall regulatory architecture.'*

[6] See recital 130 of the Proposal for a Regulation on payment services in the internal market and amending Regulation (EU) No 1093/2010, 28.06.2023 (2023/0210 (COD)): 'The *effectiveness of the Union framework for payment services depends on cooperation between multiple competent authorities, including national authorities responsible for taxation, data protection, competition, consumer protection, audit, police and other law enforcement authorities. Member States should ensure that their legal framework allows and facilitates such cooperation as necessary to achieve the objectives of the Union framework on payment services, including through the proper application of its rules.* [...]'

1. The principle of retention limitation

8. According to Article 5.1(e) GDPR, personal data "shall *be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed."*

   It is also apparent from recital 39 of the GDPR that 'personal *data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the data retention period is limited to the strict minimum. Personal data should only be processed if the purpose of the processing cannot reasonably be achieved by other means. In order to ensure that data are not retained for longer than necessary, time limits should be set by the controller for erasure or periodic review. All reasonable steps should be taken to ensure that personal data that are inaccurate are rectified or deleted.';*

9. As regards the adequacy, relevance and limitation of what is necessary for the purposes of the processing, it is necessary to recall the clarifications provided by the EDPS concerning the precision of the purposes of the processing undertaken by a controller:

   '40. A controller must determine the appropriate legal basis for the envisaged processing operations before proceeding with the processing of the data. ***Where Article 6(1)(b) forms the basis for all or part of the processing activities, the controller should anticipate what will happen in the event of termination of the contract.***

   [...]

   43. Article 17(1)(a) provides that personal data shall be erased when they are no longer necessary for the purposes for which they were collected. However, this rule does not apply if the processing is necessary for certain specific purposes, including compliance with a legal obligation under Article 17(3)(b) or the establishment, exercise or defence of legal claims under Article 17(3)(e). In practice, ***if controllers identify a general need to keep records for legal purposes, they must determine a legal basis for such retention from the beginning of the processing, and must clearly communicate, at the same time, the period for which they plan to keep the records for such legal purposes after termination of the contract.*** *In this case, they are not obliged to erase the data after termination of the contract.*

   44. In any event, ***it is possible that several processing operations with different purposes and legal bases have been identified from the start of the processing operation.*** *As long as these other processing operations remain lawful and the controller has clearly communicated these operations at the beginning of the processing, in accordance with the transparency obligations of the GDPR, it will still be possible to process personal data concerning the person for these distinct purposes after termination of the contract."*[7]

10. Once the purpose(s) of the processing has been achieved, the retention of certain data for compliance with legal obligations or for pre-litigation or litigation purposes is therefore

[7] EDPS, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, Adopted on 8 October 2019

possible, but the data must then be archived, for a period not exceeding that necessary for the purposes for which they are retained, in accordance with the provisions in force.

11. In the context of a contractual relationship between the data subject and a payment service provider, two phases in the life cycle of the user's personal data should be distinguished:

    (i) **The active phase:** the retention of the customer's personal data for the duration of the contractual relationship, mainly on the basis of the need for processing for the performance of a contract to which the data subject is a party or for the execution of pre-contractual measures taken at the request of the data subject (Article 6.1(b) GDPR), the need to comply with a legal obligation (Article 6.1(c) GDPR) or, more exceptionally, on another legal basis provided for in Article 6 GDPR, such as the data subject's consent (Article 6.1(a) GDPR) or the legitimate interest of the controller (Article 6.1(f) GDPR) (this will be referred to as the 'current use' phase of personal data);

    (ii) **The archiving phase:** the retention or 'archiving' of the customer's personal data after the end of the contractual relationship (corresponding in practice to the closure of the user's account), most often on the basis of the need to comply with a legal obligation (Article 6.1(c) GDPR) or, more exceptionally, on another legal basis provided for in Article 6 GDPR (e.g. the legitimate interest of the controller, provided for in Article 6.1(f) GDPR).

12. When the retention period for archiving is exceeded, the controller must delete the personal data (which is a right of the data subject pursuant to Article 17 GDPR). It can, for example, destroy them permanently or anonymize them.

These guidelines focus on the application of the principle of data retention limitation in archiving. Whenever a retention period is referred to in this document, it will be the second phase of the data life cycle, i.e. the archiving phase following the closure of a customer's account).

13. In accordance with the principle of accountability set out in Article 5.2 GDPR, any controller must be able to demonstrate that all the principles of Article 5.1 GDPR are complied with (including the data minimisation principle of Article 5.1(c) and the retention limitation principle of Article 5.1(e)). To this end, the controller must implement appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for each specific purpose of processing are processed within the retention period (Article 25.2 d GDPR). To this end, the data controller will have to define precisely the starting point of each retention period in order to be able to automatically comply with this obligation without waiting for a request for erasure from the data subject.

14. In order to define as precisely as possible the retention period of each set of personal data that it processes and the starting point of that period, the controller must:
    - define precisely the purposes pursued (it is not possible to keep the data 'in case ...') as well as the applicable bases of lawfulness, and
    - determine, on the basis of each specific purpose, an appropriate and necessary retention period in order to achieve that purpose.

15. If the data are used in several processing operations for more than one purpose, the storage periods must be individualised for each specific purpose.

To be noted: The controller must define the retention period or the arrangements for calculating the retention period **for each data processing** operation.

The absence of a retention period or an unlimited retention period constitutes an infringement of the GDPR. The same personal data may be used for separate processing operations and may therefore be necessary for different periods of time. The end of a data processing operation for which a data has been used does not therefore imply that the data must be erased, if it is still necessary for another ongoing data processing operation.

In such a case, it is necessary to make a clear distinction between the various data processing activities and to apply to each a period that is relevant to their respective purposes. Thus, the data associated with the longest duration will be retained and will not be deleted at the end of the first processing.

Example 1: In the context of its contractual relationship with a data subject, a payment service provider shall retain its telephone number for the purposes of authentication or communication with the data subject in the context of its contract. Once the contract is terminated, the processing of this data is no longer necessary for the performance of the contract and the payment service provider will have to erase it (unless it demonstrates that the processing of the user's telephone number is necessary for certain specific purposes, including compliance with a legal obligation under Article 17.3(b) or the establishment, exercise or defence of legal claims under Article 17.3(e).

Example 2: A payment service provider shall also process the postal address of the main residence of the data subject. This data is processed for various purposes related to the management of the relationship with the customer but also within the framework of the due diligence obligations of the payment service provider provided for by the Law of 12 November 2004 on the fight against money laundering and the financing of terrorism, as amended (the "2004 Law"). Article 3.6 of that law lays down an obligation to retain the data collected in the context of customer due diligence measures for five years after the end of the business relationship with the customer or after the date of the transaction concluded on an occasional basis. It will therefore be necessary to retain the longest storage period, and it will not be necessary to delete the address of the data subject upon termination of the contract (the date on which certain purposes of the processing of the address disappear) but rather five years after the end of the contract.

2. Definition of the basis of lawfulness for retention and of the retention period

a. Article 6.1(c) GDPR: retention necessary for compliance with a legal obligation

Article 6.1. (c) GDPR provides for the lawfulness of processing if such processing "is *necessary for compliance with a legal obligation to which the controller is subject".* In general, retention periods should, in principle, not exceed statutory limitation periods.

i. Ten-year shelf life (Commercial Code)

16. Article 16 of the Commercial Code requires traders to keep the documents or information referred to in Articles 11, 12, 14 and 15 'for *10 years from the end of the financial year to which they relate',* but only for accounting purposes. Therefore, all personal data of a customer processed in the context of accounting (records, books and records), letters received and copies of letters sent may be kept by the controller for a period of 10 years from the end of the financial year to which they relate (which generally coincides with the end of the calendar year). Personal data stored on the basis of this provision must therefore be erased at regular intervals, unless they are also processed for another purpose (e.g. compliance with another legal obligation providing for a longer retention period). Personal data collected in the context of the accounting year 2024 will therefore have to be erased or anonymised by the controller on[1] January 2035, even if the account of the data subject has still not been closed.

Example 3: A bank customer's account order may be kept for 10 years after the account has been closed. On the other hand, the copy of his identity card which was collected as part of the bank's obligations under the 2004 Act, and which is not processed by the bank as part of its accounting, will have to be deleted five years after the closure of the customer's account (unless the bank is able to demonstrate that an extended retention period of five additional years is necessary for the effective implementation of internal measures to prevent or detect acts of money laundering or terrorist financing in accordance with Article 3.6 of the aforementioned Act).

17. Furthermore, Article 27 (entitled 'Archiving') of the 2009 Law requires payment institutions and electronic money institutions to 'keep, *in accordance with the time limits laid down in the Commercial Code, all appropriate records to enable the CSSF to check that they comply with their obligations under this Law'.*

18. Moreover, if reference is made to the Law of 5 April 1993 on the financial sector as amended, credit institutions must provide for the registration and retention, in accordance with the time limits laid down in the Commercial Code, *of 'any service provided, any activity carried out and any transaction carried out by them'* (Article 37-1(6)). Data collected and stored based on the abovementioned national provisions may therefore in principle be kept

for a maximum **of 10 years from the end of the financial year to which they relate** and then be erased or anonymised by the controller (unless there is another longer retention period applicable to such data).

ii. Data retention period for the purpose of combating money laundering and terrorist financing (Law 2004)

19. In accordance with Article 3.6 of the 2004 Law, Article 1.5 of the Grand-Ducal Regulation of 1 February 2010 specifying certain provisions of the amended Law of 12 November 2004 on the fight against money laundering and terrorist financing and Article 25 of the CSSF Regulation No 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing, as amended (hereinafter "the CSSF Regulation"), professionals are required to keep for five years after the end of the business relationship with the customer or after the date of the transaction concluded on an occasional basis the following documents, data and information:
    - a copy of the documents, data and information that are necessary to comply with the customer due diligence obligations set out in sections 3 to 3-3 of the 2004 Act, the books of accounts, commercial correspondence and the results of any analysis carried out,
    - supporting documents and transaction records that are necessary to identify or reconstruct individual transactions in order to provide, where necessary, evidence in the context of a criminal investigation or investigation.

20. The CNPD notes that the personal data retained are, for example, those contained in official customer identification documents such as passports, identity cards, driving licences or other similar documents or copies of those documents; research to establish the context and purpose of abnormally large complex transactions; beneficial ownership data (e.g. extracted from the beneficial ownership register), etc.

21. The CNPD also notes that the retention of certain data on the basis of the aforementioned provisions may, in rarer cases, also concern special categories of personal data within the meaning of Article 9 of the GDPR or personal data relating to criminal convictions and offences within the meaning of Article 10 of the GDPR.[8]

22. Indeed, political opinions and religious beliefs can be revealed through financial transactions, for example, through donations made to political parties or organizations, churches or parishes. Membership of a trade union can be revealed by levying an annual fee on a person's bank account. Personal data concerning health can be obtained by analysing medical bills paid by a data subject to a health professional (e.g. a psychiatrist).

[8] Council of Europe, Advisory Committee to the Convention for the Protection of Individuals with regard to the Processing of Personal Data, Convention 108, Guidelines on the protection of personal data in the processing of personal data in the field of anti-money laundering and countering the financing of terrorism (p.20)

Finally, information about certain purchases may reveal information about a person's sex life or sexual orientation.[9]

23. Furthermore, the due diligence obligations under the 2004 Law could lead controllers to collect and store data relating to judicial proceedings against a natural person, such as those relating to his indictment or trial, and, where applicable, the resulting conviction, which constitute data relating to 'offences' and 'criminal convictions' within the meaning of Article 10 of the GDPR, irrespective of whether or not, in the course of those judicial proceedings, the commission of the offence for which the person was being prosecuted was actually established.[10]

24. Given that the context in which this type of data is processed could give rise to significant risks to the fundamental rights and freedoms of data subjects,[11]the processing of data covered by Articles 9 and 10 of the GDPR requires the controller to put in place a number of additional safeguards, such as specific information that these categories of data may be processed for the purposes of compliance with the 2004 Law or a mechanism enabling the controller to ensure that the data come from reliable sources, are accurate and up-to-date.[12]

25. Entities subject to the 2004 Act may retain their customers' personal data for an additional period of five years "where *such retention is necessary for the effective implementation of internal measures to prevent or detect money laundering or terrorist financing.* (Article 3.6(6)) or where an additional retention period is required by the supervisory authorities (Article 3.6(5)). In accordance with that provision, the CNPD points out that a period of 10 years should not be the 'default' retention period for all customers of a payment service provider. It is up to the controller, in accordance with the principle of accountability, to document why an additional period of five years is necessary.

26. It is also important to note that the 2004 Act provides that '[w]ithout *prejudice to the longer retention periods prescribed by other laws, professionals are required to erase personal data at the end of the retention periods referred to in paragraph 1 .'* (Article 3.6, paragraph 4). The obligation to erase the data of the data subjects after 5 or 10 years (after the end of the business relationship with the customer or after the date of the transaction concluded on an occasional basis) is therefore also laid down in the 2004 Law. It follows that controllers should therefore not retain data beyond these time limits for anti-money laundering and terrorist financing purposes.

---

[9] EDPS, Guidelines 6/2020 on the interaction between the Second Payment Services Directive and the GDPR, Version 2.0, adopted on 15 December 2020 (§52); European Data Protection Supervisor, Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the internal market, adopted on 22 August 2023 (§24).

[10] Judgment of 24 September 2019, GC and Others (Delisting of sensitive data), C-136/17, EU:C:2019:773, paragraph 72.

[11] See recital (51) of the GDPR.

[12] The CNPD invites controllers to read Article 76 of Regulation 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, which lays down the conditions for the processing of data referred to in Articles 9 and 10 of the GDPR (although this provision is not yet applicable, it could already serve as a 'standard' for the professionals concerned).

To be noted: Where a legal obligation requires the controller to erase the data, it may not retain the data collected for compliance with that legal obligation beyond the statutory retention period on the basis of its legitimate interest.

27. The CNPD also takes note of Article 11.2 of the CSSF Regulation, as amended, according to which: 'The *customer acceptance policy must also provide for the procedures to be followed in the event of a suspicion or reasonable grounds for suspicion of money laundering, an associated predicate offence or terrorist financing in the event of failure to contact a potential customer. The reasons for a refusal on the part of the customer or the trader to enter into a business relationship or to carry out a transaction must be documented and kept in accordance with the procedures laid down in Article 25 of this Regulation, even if the refusal on the part of the trader does not result from the finding of an indication of money laundering or terrorist financing.'* Consequently, the data of a data subject who is refused the opening of an account or himself renounces such opening may be retained in accordance with the rules laid down in the 2004 Act.

28. In the light of the foregoing, the CNPD draws a distinction between three possible starting points for calculating the retention periods prescribed by Article 3.6 of the 2004 Law:
    (i) the end of the business relationship with the customer (which corresponds, for example, to the closure of the bank account or online account of a data subject);
    (ii) the date of an occasional transaction;
    (iii) the date on which the customer or trader refused to enter into a business relationship.

29. The CNPD notes that it may happen that an account is blocked by the controller for reasons relating to the application of the 2004 Act (for example, in accordance with section 3.4 of the 2004 Act pending identity verification) and that in the event of no reaction on the part of the customer, the account remains indefinitely blocked and does not allow a retention period to be triggered. As this situation may lead in some cases to the retention of the data subject's data for an unlimited period of time in breach of Article 5.1(e) of the GDPR,[13] the CNPD recommends that the controllers concerned set up a mechanism to relaunch the data subject and close the account no later than one year after the account has been blocked (in any event, the personal data are retained following closure for anti-money laundering and counter-terrorism purposes).

iii. Special retention periods for the purpose of combating money laundering and terrorist financing (Reg. EU 2023/1113)

30. Article 26.1 of Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 recalls that information on the payer and the payee or on the originator and the payee of crypto-assets (such as, inter alia, name, payment account number, address, official identity document number, customer identification number, date and place of birth) shall not be retained beyond what is strictly necessary. The payment service provider must therefore retain such data for a period of five years, after which it must delete them (as specified in Article 26.2), unless national law provides

[13] And the requirements of section 3.4 of the 2004 Act.

otherwise specifying the circumstances in which payment service providers may or must extend the retention period for such data. Since the personal data processed by payment service providers on the basis of this Regulation are processed only for the purposes of preventing money laundering and terrorist financing (Article 25.2), the CNPD understands that the starting point of the aforementioned retention period is the same as that for the processing operations provided for by the 2004 Law, namely the end of the business relationship with the customer or the date of the transaction concluded on an occasional basis.

Example 4: an online bank processes the number of its client's official identity document in accordance with Article 26.1 of Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 and the provisions of the 2004 Act. This data must be deleted 5 years after the closure of the account of the person concerned.

iv. Recording of telephone conversations and electronic communications

31. Recording of telephone conversations and electronic communications is, in principle, possible only in accordance with the amended Law of 30 May 2005 on the protection of privacy in the electronic communications sector ('the 2005 Law') and the GDPR.

32. Thus, pursuant to section 4.3(d) of the 2005 Act, communications may be recorded:
    - based on the prior, free, specific, informed and unambiguous consent of the customer; or
    - when carried out in the context of lawful business uses, to provide evidence of a commercial transaction or other commercial communication.

33. The exception for 'commercial *communications'* may cover, for example, recordings of telephone conversations made by *call centres, help desks,* after-sales services, etc.

34. In both cases, it is necessary to inform customers and employees in advance and in a transparent manner, in particular about the purpose(s) of the registration and the retention period. This information must comply with the requirements of the GDPR.[14]

35. In order to comply with these requirements, the CNPD considers it necessary that during each telephone interview subject to surveillance, correspondents are specifically made aware of the recording, whether or not an automated message is broadcast at the beginning of the call.

36. As regards more specifically credit institutions, Article 37-1 (paragraph 6a) of the Law of 5 April 1993 on the financial sector, as amended, *lays down the obligation to keep records of telephone conversations or electronic communications 'in connection, at least, with*

[14] See Articles 12, 13 and 14 GDPR. For more information, see the CNPD's website, 'the right to information', available at https://cnpd.public.lu/en/individuals/your-rights/right-a-information.html.

transactions concluded in the context of proprietary trading and the provision of services relating to client orders concerning the receipt, transmission and execution of client orders' for 'five years and, where the CSSF so requests, for a period of up to seven years.' Telephone conversations and electronic communications must therefore in principle be deleted five years after their registration, unless longer retention is justified by another purpose compatible with the original purpose and one of the grounds for lawfulness laid down in Article 6 of the GDPR is applicable.

v. Collection of identity cards in the exercise of data subjects' rights

37. In accordance with Article 12.6 of the GDPR, where the controller has reasonable doubts as to the identity of the natural person making the request referred to in Articles 15 to 21 (for example, a request for access or erasure), it may request that additional information necessary to confirm the identity of the data subject be provided.

38. In general, the identity card should not be considered as an appropriate means of authentication to confirm the identity of the data subject unless a proportionality assessment demonstrates otherwise. Such a proportionality assessment must take account of the type of data processed, the nature of the request and the context of the request, while avoiding excessive data collection and ensuring an adequate level of security of processing[15].

39. Nevertheless, a payment service provider may ask a data subject wishing to exercise their rights under the GDPR to provide a copy of their identity card or other official document proving their identity (where such collection is justified and proportionate under the GDPR). In such a situation, the controller must then implement safeguards to prevent unauthorised or unlawful processing of the identity card. This may include refraining from making a copy after verifying the identity card or deleting a copy of an identity document immediately after successful authentication of the identity of the person concerned. Moreover, the EDPS recalled that "the subsequent *retention of a copy of an identity document may constitute a breach of the principles of purpose limitation and storage limitation (Article 5(1)(b) and (e) GDPR) and, in addition, of national law relating to the processing of the national identification number (Article 87 GDPR). The EDPB recommends, as a good practice, that the controller, after verifying the identity card, makes a note, stating for example "the identity card has been verified" in order to avoid unnecessary copying or storage of copies of identity cards."* [16]

40. The CNPD also points out that the processing of an identity card for authentication purposes in the context of the exercise of the rights of data subjects is without prejudice to the obligations to retain a copy of the identity card under the 2004 Law (the erasure of the identity card collected to confirm the identity of a person exercising, for example, a right of access in accordance with Article 15 of the GDPR, does not presuppose the erasure of his

[15] EDPB, Guidelines 01/2022 on the rights of data subjects – Right of access, Version 2.1, adopted on 28 March 2023 (§70-77)
[16] EDPB, Guidelines 01/2022 on the rights of data subjects – Right of access, Version 2.1, adopted on 28 March 2023 (§79 and the case-law cited)

identity card retained for purposes related to the fight against money laundering and terrorist financing ('AML/CFT') in a separate database).[17]

b. Article 6.1(f) GDPR: retention necessary for the purposes of the controller's legitimate interests

i. Reminder of the conditions for the use of legitimate interest

41. Article 6.1(f) GDPR provides for the lawfulness of processing if such processing "is *necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child, prevail".*

42. The CNPD would like to recall the three cumulative conditions for a controller to be able to rely on Article 6.1(f) GDPR:[18]
    i) the pursuit of a legitimate interest by the controller or by a third party;
    ii) the necessity of the processing of personal data for the fulfilment of the legitimate interest pursued (the legitimate interest in the processing of data pursued cannot reasonably be achieved as effectively by other means less detrimental to the fundamental rights and freedoms of the data subjects);
    iii) the interests or fundamental rights and freedoms of the data subject do not override the legitimate interest of the controller or a third party (e.g. where personal data are processed in circumstances where data subjects do not reasonably expect such processing).

43. The conditions for the application of the legitimate interest must be interpreted restrictively.[19] Legitimate interest must not constitute a basis for lawfulness by default. The CNPD recommends a balancing of the rights and interests involved for each processing operation, which analysis must be detailed and documented before the processing operation in question.

44. This involves assessing the degree of intrusion of the envisaged processing into the individual sphere, by measuring its impact on the privacy of individuals (processing of sensitive data, processing of vulnerable persons, profiling, etc.) and on their other fundamental rights (freedom of expression, freedom of information, freedom of conscience, etc.) as well as the other concrete impacts of the processing on their situation (monitoring or surveillance of their activities, banking exclusion, etc.). Those impacts must be measured in order to determine, on a case-by-case basis, the extent of the intrusion caused by the processing into the lives of individuals.[20]

---

[17] See point 2.a.iii
[18] Judgment of 4 July 2023, C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), paragraph 106
[19] Judgment of 4 July 2023, Meta Platforms and Others (General conditions of use of a social network), C-252/21, ECLI:EU:C:2023:537, paragraphs 92 and 93 and the case-law cited
[20] Judgment of 4 July 2023, C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), paragraphs 116 and 118.

45. Recourse to this legal basis entails certain additional obligations for the controller in managing the rights of data subjects:
    - Specific obligation to provide information on the legitimate interests pursued (Article 13.1(d) GDPR where the personal data are collected from the data subject and Article 14.2(b) GDPR where the personal data have not been collected from the data subject);
    - Right of objection of the data subject (Article 21(1) of the GDPR): right of the data subject to object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him or her based on legitimate interest, including profiling based on those provisions. The controller shall no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims;
    - Right to restriction of processing (Article 18 GDPR): right of the data subject to obtain the restriction of processing where the data subject has objected to the processing pursuant to Article 21.1 GDPR, during the verification of whether the legitimate grounds pursued by the controller outweigh those of the data subject.

46. For further details on the criteria that controllers must fulfil in order to process personal data on the basis of legitimate interest, the CNPD invites relevant actors to read the draft EDPS guidelines on legitimate interest[21].

47. In the following sections, the CNPD will analyse purposes that could be pursued on the basis of the legitimate interest of a payment service provider.

ii. Retention of data necessary for the establishment, exercise or defence of legal claims

48. Recital 65 of the GDPR specifies that the further storage of personal data should be lawful where it is necessary for the establishment, exercise or defence of legal claims. In that context, limitation periods may therefore provide important guidance for determining shelf-life.[22]

49. Article 189 of the Commercial Code provides that 'obligations *arising in the course of trade between traders or between traders and non-traders shall be prescribed by 10 years if they are not subject to shorter requirements'.* It is therefore possible for a payment service provider to retain any personal data that it may need in the context of a dispute with the customer. Only personal data in connection with the performance of contracts and the services provided by the controller shall be retained for this purpose.

Example 5: Only the data necessary for the performance of the contract between a bank and its customer (for example, a statement of account) may be retained after the closure of the

[21] *EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Adopted on 8 October 2024* (this version of the guidelines is subject to public consultation).
[22] Opinion of the National Data Protection Commission on Draft Law No 7945 transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, Deliberation No 49AV25/2022 of 21 October 2022 (p.22)

account of the person concerned in order to constitute evidence in the event of litigation, within the limitation period of Article 189 of the Commercial Code (10 years). On the other hand, data collected as part of the bank's *due diligence obligations under the 2004 Law, such as data collected from 'watchlists', must be deleted after 5 years (in the absence of an extended retention* period of 5 years),in accordance with Article 3.6(4) of the 2004 Law ('Without prejudice *to the longer retention periods prescribed by other laws, professionals are required to erase personal data at the end of the retention periods referred to in subparagraph 1')*and Article 3.6bis(2) ('Processing of personal data on the basis of this Law for any other purpose is prohibited').

iii. Retention of customer data for fraud prevention purposes

50. Fraud prevention is identified in Recital 47 GDPR as one of the possible legitimate interests protected by Article 6.1(f) GDPR.

51. With regard more specifically to payment service providers, it is worth recalling the provisions of Article 105 of the 2009 Law: 'Payment *systems and payment service providers shall be entitled to process personal data where necessary to ensure the prevention, investigation and detection of payment fraud. ...*'.[23]

52. In the context of its Guidelines on the interaction between the Second Payment Services Directive and the GDPR,[24] the EDPS recalled that the processing of personal data strictly necessary for fraud prevention purposes may constitute a legitimate interest of the payment service provider concerned, provided that the interests or fundamental rights and freedoms of the data subject do not override those interests. Processing activities for fraud prevention purposes should then be based on a thorough case-by-case assessment by the controller, in line with the principle of accountability.

53. Furthermore, the EDPS indicated in his guidelines on legitimate interest that the processing of personal data in the context of the legitimate interest of fraud prevention does not apply without conditions and limitations, in particular because this type of processing can have a significant impact on data subjects. For example, recital 47 of the GDPR specifies that the processing of personal data must be "strictly *necessary for fraud prevention purposes",* which must be considered in conjunction with the principle of data minimisation enshrined in Article 5.1(c) of the GDPR. The EDPS also states that, at the same time, the principle of storage limitation, laid down in Article 5.1(e) of the GDPR, must

[23] It is likely that the basis of lawfulness for this type of processing will in the future be the legal obligation (Article 6.1(c) GDPR): cf. Article 83 of the Proposal for a Regulation on payment services in the internal market and amending Regulation (EU) No 1093/2010. It is interesting to note that Article 83 of the Proposal provides: 'Payment *service providers shall not store the data referred to in this paragraph for longer than necessary for the purposes set out in paragraph 1 or after the termination of the relationship with the customer*.';

[24] Guidelines 6/2020 on the interaction between the Second Payment Services Directive and the GDPR, version 2.0, adopted on 15 December 2020

be taken into account when defining data retention policies applicable to data processed for fraud detection or prevention purposes.[25]

54. In practice, the processing carried out for control and anti-fraud purposes results in profiling using algorithms that use all available data to calculate a fraud or error risk rate for each customer (e.g. based on a history of fraud already committed). While fully recognizing the importance of the fight against payment fraud, the CNPD nevertheless wishes to reiterate the great caution with which these algorithms must be designed and used, given the risks they present and the biases they may be subject to.

55. In an online context, this type of processing may involve the collection of transaction data but also data related to the context of a payment transaction such as behavioural data (behavioral analysis such as keystroke dynamics, data related to purchasing and consumption habits), navigation data and data relating to connection to information systems (geolocation data, data relating to equipment: IP address, screen or browser setting, etc.).

56. The prevention, investigation and detection of payment fraud may involve different types of processing such as the detection of anomaly or inconsistency, the management and analysis of such alerts, the compilation of lists of persons duly identified as perpetrators of acts qualified as fraud or attempted fraud as such by the controller. These processing operations can be described as 'profiling' within the meaning of the GDPR.[26] While there may be benefits to retaining data in the case of profiling, as there will be more data that the algorithm can learn from, controllers must respect the principle of data minimisation when collecting personal data and ensure that they retain such personal data only for as long as is necessary and proportionate to the purposes for which the data are processed.[27]

57. In the light of the foregoing, the CNPD considers that the retention period for data in the context of the prevention and detection of fraud should be limited to the time strictly necessary for the accomplishment of that purpose. For example, the retention of data of a data subject for whom no fraud has been detected during the duration of the contract after the closure of his or her account does not seem necessary or proportionate. In this case, the CNPD considers that the controller should erase (or anonymize) the data processed to fight fraud after the end of the contractual relationship with the customer.

---

[25] *EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Adopted on 8 October 2024*, paragraph 104 (this version of the guidelines is subject to public consultation).

[26] Profiling is defined as "any *form of automated processing of personal data aimed at assessing the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, or location and movements, where it produces legal effects concerning the data subject or significantly affects him or her in a similar way"* (para. 71 GDPR).

[27] See Article 29 Data Protection Working Party, Guidelines on automated individual decision-making and profiling for the purposes of Regulation (EU) 2016/679 (WP251rev.01, p.13).

3. Good practices in the implementation of the retention limitation principle

58. In accordance with Articles 5 and 25 of the GDPR, the controller must implement appropriate technical and organisational measures, which are intended to implement the data protection principles effectively and to accompany the processing with the necessary safeguards in order to meet the requirements of the GDPR, including appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for each specific purpose of the processing are processed.

a. Establishment of a data sorting mechanism

59. Thus, the controller must put in place measures to sort the processed data once the current phase of use of the data subject's data has ended (which coincides, for example, with the closure of the user's account) in order to retain only those personal data that are relevant in view of the (new) purposes in the context of the archiving phase. The systematic and indiscriminate retention of all data in an account after the end of the contractual relationship with the data subject does not comply with the principle of limitation of retention.[28] This 'purging' mechanism may result in the erasure or anonymisation of personal data which are not necessary for the purposes of data retention.

60. The controller should thus provide for the storage of the data in a database dedicated to archiving (a) or at least provide for logical separation in the active database (b)29.
    (a) A physical separation could be made by extracting data from the information system to keep them separately in a dedicated archiving database to which only specifically authorised persons will be able to access. In this case, the archiving database will have to include different functionalities, such as exporting, accessing and viewing stored data. These functionalities will allow the organisation to be able to respond to the data subject when exercising their rights (right of access, etc.).

    (b) With a logical separation, the data remain in the 'active database' but are clearly identified and isolated from other data by limiting the authorisations in order to make them inaccessible to persons who no longer need to process them.[30]

b. Establishment of a mechanism for closing "inactive" accounts

61. Some players offer their financial services only through the creation of an online account. The CNPD notes that it is often the case that these users no longer use these accounts, without closing them, which sometimes leads to the existence of inactive

[28] Article 5.1(e) GDPR. See Commission Nationale de l'Informatique et des Libertés, Deliberation of restricted training No SAN-2024-002 of 31 January 2024 concerning the company DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS
[29] See Commission Nationale de l'Informatique et des Libertés, Deliberation of restricted training No SAN-2022-018 of 8 September 2022 concerning the GIE INFOGREFFE
[30] See the CNIL's practical guide on storage periods.

accounts for an indefinite period, the absence of closure thus preventing certain retention periods from running. Thanks to the law of 30 March 2022 on inactive accounts, inactive safes and dormant insurance contracts, which entered into force on 1 June 2022, Luxembourg has established for the first time a legal framework for the management of inactive accounts. The new legal framework is applicable to "any *sight account, savings account, term or redeemable deposit account with notice, securities account, fiduciary deposit as well as any other accounts opened with an institution."* By contrast, electronic money accounts within the meaning of the amended Law of 10 November 2009 on payment services are excluded from the scope of that legal framework.

62. In order to ensure that processing is accompanied by the necessary safeguards to meet the requirements of the GDPR, including the principle of accuracy and storage limitation, controllers should provide for measures to verify on a regular basis that the account holder is still willing to maintain the account online and that the data stored therein is accurate. In the case of accounts where the balance is at zero, the CNPD also recommends establishing a deadline at the end of which the account will be considered inactive and must be closed (after informing the person concerned). In that regard, the CNPD considers that a period of five years appears proportionate.[31]

[31] This recommendation is without prejudice to the provisions laid down in the Law of 30 March 2022 on inactive accounts, inactive safes and dormant insurance contracts.

4. The obligation to inform data subjects about retention periods

63. Pursuant to Article 12 GDPR, the controller must provide data subjects with information relating to the processing carried out "in *a concise, transparent, intelligible and easily accessible manner, in clear and plain language [...]"*when communicating with data subjects.

a. Right to prior information

Articles 13.2(a) (Information to be provided where personal data are collected from the data subject) and 14.2(a) of the GDPR (Information to be provided where the personal data have not been collected from the data subject) require the controller to inform individuals about the period of retention of the data (or, where that is not possible, the criteria used to determine that period). Accurate information on retention periods, in so far as they help to ensure that data subjects have control over the processing of their data, is important in order to ensure fair and transparent processing.[32]

64. In view of these provisions, the CNPD recalls that payment service providers must be transparent about the retention periods of users' personal data, in particular following the closure of their account. This also implies information on the bases of lawfulness applied for the retention of their data (the determination of these bases of lawfulness making it possible, in particular, to determine their rights provided for by the GDPR). In the case of Article 6.1(f) GDPR, the nature of the legitimate interest pursued by the controller should be included in the information brought to the attention of individuals. Moreover, the obligation of transparency is reinforced when it comes to the processing of special categories of personal data referred to in Articles 9 and 10 of the GDPR.[33]

b. Right to information when exercising rights under processing

65. The controller must also provide clear information to data subjects when exercising their rights, such as rights of access and erasure (Article 12.1 GDPR).

66. When a data subject contacts a payment service provider in the exercise of his or her GDPR rights and if the data subject has questions relating to the retention of his or her data (e.g. a request for erasure), the controller must then be able to provide precise information: purpose(s) of storage, basis(s) of lawfulness, event triggering the storage

[32] See Commission Nationale de l'Informatique et des Libertés, Deliberation of restricted training No SAN-2024-002 of 31 January 2024 concerning the company DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS
[33] Footnote LDT EDPB Transparency

period, exact date(s) of erasure, data that can be erased and data to be retained (information already included in the payment service provider's processing register).

Example 6: A user (data subject) makes a request to erase all his/her data (on the basis of Article 17(1)(a) GDPR) to a payment service provider after terminating his/her contract with him/her. The payment service provider, acting as data controller, will not be able to erase a large part of the data subject's data in view of the legal obligations applicable to it (Article 17.3(b) GDPR). In its reply to the data subject, the information provided by the controller must then, in accordance with Article 12.1 of the GDPR, be more specific than in its information notice and must, in particular, contain developments relating to the applicable legal provisions and the categories of data that cannot be deleted. A mere reference to the 'legal obligations applicable in the financial sector' cannot be regarded as sufficient in the light of Article 12(1) of the GDPR.

Example 7: During the archiving phase, a user (data subject) objects, on the basis of Article 21(1) of the GDPR and for reasons relating to his or her particular situation, to the processing of his or her data on the basis of the legitimate interest of the PSP. After possibly restricting the processing pursuant to Article 18(1)(d) GDPR, the controller will have to either **(i)** erase the data pursuant to Article 17(1)(c) GDPR or **(ii)** demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims (Article 21(1) GDPR). It is in those circumstances that it is for the payment service provider to provide the data subject with precise information about the processing and, in particular, about the overriding legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.