Die Datenschutz-Grundverordnung

Leitlinien zu den Aufbewahrungsfristen für personenbezogene Daten durch Zahlungsdienstleister

Datum der ersten Annahme: 06/06/2025

Inhaltsverzeichnis

Einleitung

1. Diese Leitlinien richten sich in erster Linie an Zahlungsdienstleister (im Folgenden: Zahlungsdienstleister (ZDL) oder Verantwortliche) im Sinne des abgeänderten Gesetzes vom 10. November 2009 über Zahlungsdienste[1] (im Folgenden: Gesetz von 2009).[2]

2. Die Zahlungsdienstleister erheben und verarbeiten zum Zeitpunkt der Kontaktaufnahme, während der gesamten Dauer der Beziehung und auch lange nach Beendigung der Beziehung mit dem Nutzer des Dienstes (im Folgenden: Nutzer oder betroffene Person) eine erhebliche Menge personenbezogener Daten. Darüber hinaus haben technologische Innovationen die Fähigkeit der Zahlungsdienstleister, ein breites Spektrum von Nutzerdaten zu erfassen, zu speichern, zu kombinieren und zu analysieren, erheblich verbessert.

3. Personenbezogene Daten, die von Zahlungsdienstleistern verarbeitet werden können, können Informationen über die persönliche Situation der betroffenen Person (Alter, Staatsangehörigkeit, Familienstand usw.), ihre wirtschaftliche und finanzielle Situation, Zahlungsdaten (wie Transaktionsbetrag, Datum und Uhrzeit der Zahlung, Identität des Empfängers einer Transaktion, IBAN oder personalisierte Sicherheitsdaten), den Betrugsbekämpfungswert der betroffenen Person, Kontext- oder Verhaltensdaten (Konsumpräferenzen und -gewohnheiten, Geolokalisierung, Merkmale des für einen Online-Kauf verwendeten Endgeräts, Zeitaufwand für die Prospektion usw.) umfassen.

4. Obwohl ihnen nach der Datenschutz-Grundverordnung (EU) 2016/679 (im Folgenden: DSGVO) kein besonderer Status zukommt, sind viele dieser Daten als „sensible“ Daten (im allgemeinen Sinne des Wortes) anzusehen, da ihre Verletzung schwerwiegende Auswirkungen auf das tägliche Leben der betroffenen Person haben könnte.[3]

5. Angesichts des Umfangs dieser Verarbeitungen möchte die CNPD einige der wichtigsten Grundsätze von Artikel 5 der DSGVO in Bezug auf die Verarbeitung von Daten von Zahlungsdienstnutzern in Erinnerung rufen. Ein Zahlungsdienstleister darf personenbezogene Daten einer betroffenen Person nur verarbeiten, wenn die beabsichtigte Verarbeitung **rechtmäßig ist;** d. h. erforderlich für die Erfüllung des Vertrags mit dem Nutzer, erforderlich für die Erfüllung einer rechtlichen Verpflichtung, der der ZDL unterliegt, erforderlich für die Zwecke der vom ZDL verfolgten berechtigten Interessen oder in selteneren Fällen auf einer der anderen Rechtsgrundlagen für die Verarbeitung der in Artikel 6 der DSGVO genannten Daten. Nach dem Grundsatz der **Transparenz** müssen die betroffenen Personen die Kontrolle über die sie betreffenden Daten behalten. Dies setzt voraus, dass sie ab dem Zeitpunkt der Erhebung und während des gesamten Verarbeitungszyklus eindeutig über die Verwendung ihrer Daten informiert werden.

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

[2] Die in diesen Leitlinien dargelegten Grundsätze können zwar auch für andere Berufsangehörige des Finanzsektors gelten, doch sollen in dieser Leitlinie nicht die Besonderheiten dargelegt werden, die für andere Berufsangehörige gelten.

[3] Leitlinien der Artikel-29-Datenschutzgruppe zur Datenschutz-Folgenabschätzung (DSFA) und zur Feststellung, ob die Verarbeitung für die Zwecke der Verordnung (EU) 2016/679 „mit hohem Risiko verbunden sein kann“, WP248 rev.01 – vom EDSA gebilligt (S. 11); Leitlinien 6/2020 zum Zusammenspiel zwischen der Zweiten Zahlungsdiensterichtlinie und der DSGVO, Version 2.0, angenommen am 15. Dezember 2020 (§69)

Darüber hinaus dürfen die personenbezogenen Daten der Nutzer nur für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet und nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist (Grundsatz **der Zweckbindung).** Die Daten müssen außerdem angemessen, relevant und auf das für die Zwecke, für die sie verarbeitet werden, erforderliche Maß beschränkt sein (Grundsatz **der Datenminimierung).** Sie müssen auch genau sein und erforderlichenfalls auf dem neuesten Stand gehalten werden (Genauigkeitsgrundsatz).

6. Schließlich müssen nach Art. 5 Abs. 1 Buchst. e der DSGVO personenbezogene Daten „in *einer Form gespeichert werden, die die Identifizierung der betroffenen Personen für einen Zeitraum ermöglicht, der nicht länger dauert, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“* (Grundsatz **der Beschränkung der Speicherung von Daten).** In diesen Leitlinien wird nicht im Einzelnen auf die Frage eingegangen, welche Daten für die Erfüllung der Verträge erforderlich sind und während der Dauer des Vertragsverhältnisses gespeichert werden, sondern auf alle Aspekte der Aufbewahrungsfristen nach Beendigung des Vertragsverhältnisses mit der betroffenen Person. In der Tat speichern ZDLs in der Regel die personenbezogenen Daten ihrer Nutzer, um bestimmte gesetzliche Verpflichtungen zu erfüllen oder um sich vor bestimmten rechtlichen Schritten während der Dauer der gesetzlichen Vorschriften zu schützen.

7. Ohne Anspruch auf Vollständigkeit zu erheben, zielen diese Leitlinien darauf ab, die betroffenen Akteure über die Dauer und die Modalitäten der Speicherung der personenbezogenen Daten zu informieren, die sie im Kontext eines stark regulierten Sektors verarbeiten. Der Schutz personenbezogener Daten ist zunehmend in den verschiedenen europäischen Vorschriften (auch den speziell für den Finanzsektor geltenden) verankert, und die CNPD möchte die betroffenen Verantwortlichen so weit wie möglich über die Anwendung einiger dieser Bestimmungen in Bezug auf die Anforderungen der DSGVO in Bezug auf die Aufbewahrungsfristen für personenbezogene Daten informieren. Angesichts der Präsenz zahlreicher Zahlungsdienstleister, die als in Luxemburg Ansässige für die Verarbeitung Verantwortliche fungieren,[4] und im Einklang mit den Empfehlungen des Europäischen Datenschutzausschusses (im Folgenden: EDSB) und des europäischen Gesetzgebers beabsichtigt die CNPD, in Zusammenarbeit mit den anderen zuständigen Behörden in Luxemburg einen ganzheitlichen[5][6]Ansatz für den für die Akteure des Finanzsektors geltenden Rechtsrahmen zu verfolgen.

---

[4] Im Mai 2025 gab es in Luxemburg 117 Kreditinstitute, 17 Zahlungsinstitute und 12 E-Geld-Institute (Quelle: https://www.cssf.lu/wp-content/uploads/newsletter292.pdf)

[5] Siehe *EDPB Strategy 2024-2027:* „Der *EDSA wird sich bemühen, die Zusammenarbeit mit anderen Regulierungsbehörden zu verstärken, um das Recht auf Datenschutz in die gesamte Regulierungsarchitektur zu integrieren.“*

[6] Siehe Erwägungsgrund 130 des Vorschlags für eine Verordnung über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/2010, 28.06.2023 (2023/0210 (COD)): „Die *Wirksamkeit des EU-Rahmens für Zahlungsdienste hängt von der Zusammenarbeit mehrerer zuständiger Behörden ab, darunter nationale Steuer-, Datenschutz-, Wettbewerbs-, Verbraucherschutz-, Audit-, Polizei- und andere Durchsetzungsbehörden. Die Mitgliedstaaten sollten sicherstellen, dass ihr Rechtsrahmen eine solche Zusammenarbeit ermöglicht und erleichtert, soweit dies für die Verwirklichung der Ziele des Unionsrahmens für Zahlungsdienste erforderlich ist, unter anderem durch die ordnungsgemäße Anwendung seiner Vorschriften.* [...]“

1. Der Grundsatz der Speicherbegrenzung

8. Nach Art. 5 Abs. 1 Buchst. e der DSGVO *sind personenbezogene Daten „in einer Form aufzubewahren, die die Identifizierung der betroffenen Personen für einen Zeitraum ermöglicht, der nicht länger ist, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist".*

   Im 39. Erwägungsgrund der DSGVO heißt es weiter: „Personenbezogene *Daten sollten angemessen, relevant und auf das für die Zwecke, für die sie verarbeitet werden, erforderliche Maß beschränkt sein. Dies erfordert insbesondere, dass die Dauer der Datenspeicherung auf das absolute Minimum beschränkt wird. Personenbezogene Daten sollten nur verarbeitet werden, wenn der Zweck der Verarbeitung mit anderen Mitteln vernünftigerweise nicht erreicht werden kann. Um sicherzustellen, dass die Daten nicht länger als erforderlich gespeichert werden, sollte der für die Verarbeitung Verantwortliche Fristen für ihre Löschung oder für eine regelmäßige Überprüfung festlegen. Es sollten alle zumutbaren Maßnahmen getroffen werden, um sicherzustellen, dass unrichtige personenbezogene Daten berichtigt oder gelöscht werden."*

9. In Bezug auf die Angemessenheit, Relevanz und Begrenztheit dessen, was für die Zwecke der Verarbeitung erforderlich ist, ist auf die Klarstellungen hinzuweisen, die der EDSB in Bezug auf die genauen Zwecke der Verarbeitung durch einen Verantwortlichen vorgenommen hat:

   „40. Ein für die Verarbeitung Verantwortlicher muss vor der Verarbeitung der Daten die geeignete Rechtsgrundlage für die beabsichtigte Verarbeitung ermitteln. ***Wenn Artikel 6 Absatz 1 Buchstabe b die Grundlage für alle oder einen Teil der Verarbeitungstätigkeiten bildet, sollte der Verantwortliche voraussehen, was im Falle einer Kündigung des Vertrags geschehen wird.***

   [...]

   43. Nach Artikel 17 Absatz 1 Buchstabe a werden personenbezogene Daten gelöscht, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind. Dies gilt jedoch nicht, wenn die Verarbeitung für bestimmte Zwecke erforderlich ist, insbesondere zur Erfüllung einer rechtlichen Verpflichtung nach Artikel 17 Absatz 3 Buchstabe b oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen nach Artikel 17 Absatz 3 Buchstabe e. In der Praxis ***müssen die für die Verarbeitung Verantwortlichen, wenn sie einen allgemeinen Bedarf an der Aufbewahrung von Aufzeichnungen für rechtmäßige Zwecke feststellen, von Beginn der Verarbeitung an eine Rechtsgrundlage für diese Aufbewahrung festlegen und gleichzeitig klar angeben, wie lange sie beabsichtigen, die Aufzeichnungen für diese rechtmäßigen Zwecke nach Beendigung des Vertrags aufzubewahren.*** *In diesem Fall sind sie nicht verpflichtet, die Daten nach Beendigung des Vertrags zu löschen.*

   44. In jedem Fall ist ***es möglich, dass zu Beginn der Verarbeitung mehrere Verarbeitungen mit unterschiedlichen Zwecken und Rechtsgrundlagen identifiziert wurden.*** *Solange diese anderen Verarbeitungsvorgänge rechtmäßig bleiben und der Verantwortliche diese Vorgänge zu Beginn der Verarbeitung im Einklang mit den Transparenzpflichten der DSGVO eindeutig mitgeteilt hat, ist es nach Beendigung des*

Vertrags weiterhin möglich, personenbezogene Daten, die sich auf die Concerte-Person beziehen, für diese gesonderten Zwecke zu verarbeiten.[7]

10. Sobald der/die Zweck(e) der Verarbeitung erreicht ist/sind, ist es daher möglich, bestimmte Daten zur Erfüllung rechtlicher Verpflichtungen oder für vorprozessuale oder streitige Zwecke zu speichern, aber die Daten müssen dann gemäß den geltenden Bestimmungen für einen Zeitraum archiviert werden, der nicht länger ist, als es für die Zwecke, für die sie gespeichert werden, erforderlich ist.

11. Im Rahmen eines Vertragsverhältnisses zwischen der betroffenen Person und einem Zahlungsdienstleister sind im Lebenszyklus der personenbezogenen Daten des Nutzers zwei Phasen zu unterscheiden:

    (i) **Die aktive Phase:** die Speicherung personenbezogener Daten des Kunden für die Dauer des Vertragsverhältnisses, hauptsächlich auf der Grundlage der Notwendigkeit der Verarbeitung zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person getroffen werden (Art. 6.1 Buchst. b DSGVO), der Notwendigkeit der Erfüllung einer rechtlichen Verpflichtung (Art. 6.1 Buchst. c DSGVO) oder, in Ausnahmefällen, auf einer anderen Rechtsgrundlage gemäß Art. 6 DSGVO, wie der Einwilligung der betroffenen Person (Art. 6.1 Buchst. a DSGVO) oder dem berechtigten Interesse des Verantwortlichen (Art. 6.1 Buchst. f DSGVO) (hier wird von einer Phase der „üblichen Nutzung" personenbezogener Daten gesprochen);

    (ii) **Die Archivierungsphase:** die Speicherung oder „Archivierung" der personenbezogenen Daten des Kunden nach Beendigung des Vertragsverhältnisses (in der Praxis entspricht dies der Schließung des Kontos des Nutzers), meistens auf der Grundlage der Notwendigkeit der Erfüllung einer rechtlichen Verpflichtung (Artikel 6.1 Buchstabe c DSGVO) oder in Ausnahmefällen auf einer anderen Rechtsgrundlage gemäß Artikel 6 DSGVO (z. B. dem berechtigten Interesse des Verantwortlichen gemäß Artikel 6.1 Buchstabe f der DSGVO).

12. Wird die Speicherdauer im Rahmen der Archivierung überschritten, hat der Verantwortliche die Löschung der personenbezogenen Daten (ein Recht der betroffenen Person gemäß Artikel 17 der DSGVO) vorzunehmen. Er kann sie zum Beispiel endgültig vernichten oder anonymisieren.

Diese Leitlinien konzentrieren sich auf die Anwendung des Grundsatzes der Beschränkung der Vorratsdatenspeicherung im Rahmen der Archivierung. Jedes Mal, wenn in diesem Dokument auf eine Speicherdauer Bezug genommen wird, handelt es sich um die zweite Phase des Lebenszyklus der Daten, d. h. die Archivierungsphase nach Schließung des Kontos eines Kunden).

[7] EDSB, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO bei der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, angenommen am 8. Oktober 2019

13. Im Einklang mit dem in Artikel 5.2 der DSGVO verankerten Grundsatz der Rechenschaftspflicht muss jeder Verantwortliche nachweisen können, dass alle Grundsätze des Artikels 5.1 der DSGVO eingehalten werden (einschließlich des Grundsatzes der Datenminimierung gemäß Artikel 5.1 Buchstabe c und des Grundsatzes der Speicherbegrenzung gemäß Artikel 5.1 Buchstabe e). Zu diesem Zweck muss der Verantwortliche geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass standardmäßig nur die personenbezogenen Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind (Artikel 25.2 d der DSGVO). Zu diesem Zweck muss der für die Verarbeitung Verantwortliche den Beginn jeder Speicherfrist genau festlegen, damit er dieser Verpflichtung automatisch nachkommen kann, ohne auf einen Löschungsantrag der betroffenen Person zu warten.

14. Um die Speicherdauer jedes von ihm verarbeiteten Satzes personenbezogener Daten und den Beginn dieser Dauer so genau wie möglich festzulegen, muss der für die Verarbeitung Verantwortliche
    - die genauen Zwecke (es ist nicht möglich, die Daten „für den Fall ...“ aufzubewahren) und die anwendbaren Rechtmäßigkeitsgrundlagen festzulegen und
    - für jeden spezifischen Zweck eine angemessene und notwendige Speicherdauer festzulegen, um diesen Zweck zu erreichen.

15. Wenn die Daten für mehrere Verarbeitungen mit mehreren Zwecken verwendet werden, sind die Aufbewahrungsfristen für jeden spezifischen Zweck zu individualisieren.

Hervorzuheben sind: Der für die Verarbeitung Verantwortliche muss die Speicherfrist oder die Modalitäten für die Berechnung der Speicherfrist **für jede Datenverarbeitung** festlegen.

Das Fehlen einer Speicherfrist oder einer unbegrenzten Speicherfrist stellt einen Verstoß gegen die DSGVO dar. Dieselben personenbezogenen Daten können für unterschiedliche Verarbeitungen verwendet werden und können daher für unterschiedliche Zeiträume erforderlich sein. Die Beendigung einer Datenverarbeitung, für die Daten verwendet wurden, bedeutet daher nicht, dass die Daten gelöscht werden müssen, wenn sie noch für eine andere laufende Datenverarbeitung erforderlich sind.

In einem solchen Fall ist es notwendig, die verschiedenen Datenverarbeitungstätigkeiten genau zu unterscheiden und auf jede von ihnen einen Zeitraum anzuwenden, der für ihre jeweiligen Zwecke relevant ist. Auf diese Weise werden die Daten mit der längsten Dauer gespeichert und am Ende der ersten Verarbeitung nicht gelöscht.

Beispiel 1: Im Rahmen seines Vertragsverhältnisses mit einer betroffenen Person bewahrt ein Zahlungsdienstleister seine Telefonnummer für Authentifizierungszwecke oder für die Kommunikation mit dieser Person im Rahmen seines Vertrags auf. Nach Beendigung des Vertrags ist die Verarbeitung dieser Daten für die Erfüllung des Vertrags nicht mehr erforderlich, und der Zahlungsdienstleister muss sie löschen (es sei denn, er weist nach, dass die Verarbeitung der Telefonnummer des Nutzers für bestimmte Zwecke erforderlich ist, einschließlich der Erfüllung einer rechtlichen Verpflichtung gemäß Artikel 17.3 Buchstabe b oder der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen gemäß Artikel 17.3 Buchstabe e).

Beispiel 2: Ein Zahlungsdienstleister verarbeitet auch die Postanschrift des Hauptwohnsitzes der betroffenen Person. Diese Daten werden für verschiedene Zwecke im Zusammenhang mit der Verwaltung der Kundenbeziehung, aber auch im Rahmen der Sorgfaltspflichten des Zahlungsdienstleisters gemäß dem Gesetz vom 12. November 2004 zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung in seiner geänderten Fassung (das "Gesetz von 2004") verarbeitet. Art. 3.6 dieses Gesetzes sieht jedoch eine Verpflichtung vor, die im Rahmen der Sorgfaltspflichten gegenüber dem Kunden erhobenen Daten für einen Zeitraum von fünf Jahren nach Beendigung der Geschäftsbeziehung mit dem Kunden oder nach dem Zeitpunkt des gelegentlichen Geschäftsvorfalls aufzubewahren. Daher ist die längste Speicherdauer zugrunde zu legen, und es ist nicht erforderlich, die Adresse der betroffenen Person bei Vertragsbeendigung (Datum, an dem bestimmte Zwecke der Adressverarbeitung entfallen) zu löschen, sondern fünf Jahre nach Vertragsende.

2. Festlegung der Rechtsgrundlage für die Speicherung und der Speicherdauer

a. Art. 6 Abs. 1 Buchst. c der DSGVO: Speicherung zur Erfüllung einer gesetzlichen Verpflichtung erforderlich

Artikel 6.1. (c) DSGVO sieht die Rechtmäßigkeit einer Verarbeitung vor, wenn die Verarbeitung "zur *Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt".* Grundsätzlich sollten die Aufbewahrungsfristen die gesetzlichen Verjährungsfristen nicht überschreiten.

i. Zehnjährige Speicherung (Handelsgesetzbuch)

16. Art. 16 des Handelsgesetzbuchs verpflichtet die Händler, die in den Art. 11, 12, 14 und 15 genannten Unterlagen oder Informationen „zehn *Jahre ab dem Ende des Geschäftsjahres, auf das sie sich beziehen“,* aufzubewahren, jedoch nur zu Buchhaltungszwecken. Daher können alle im Rahmen der Buchhaltung verarbeiteten personenbezogenen Daten eines Kunden (Register, Bücher und Buchungsbelege), die erhaltenen Schreiben und die Kopien der versandten Schreiben vom für die Verarbeitung Verantwortlichen für einen Zeitraum von 10 Jahren ab dem Ende des Geschäftsjahres, auf das sie sich beziehen, aufbewahrt werden (was in der Regel mit dem Ende des Kalenderjahres zusammenfällt). Personenbezogene Daten, die auf der Grundlage dieser Bestimmung gespeichert werden, müssen daher in regelmäßigen Abständen gelöscht werden, es sei denn, sie werden auch zu einem anderen Zweck verarbeitet (z. B. zur Erfüllung einer anderen rechtlichen Verpflichtung, die eine längere Aufbewahrungsfrist vorsieht). Personenbezogene Daten, die im Rahmen des Geschäftsjahres 2024 erhoben wurden, müssen daher vom für die Verarbeitung Verantwortlichen am 1. Januar 2035 gelöscht oder anonymisiert werden, auch wenn das Konto der betroffenen Person noch nicht geschlossen wurde.

Beispiel 3: Der Kontobeschluss des Kunden einer Bank kann nach Schließung seines Kontos zehn Jahre lang aufbewahrt werden. Dagegen muss die Kopie ihres Personalausweises, die im Rahmen der Verpflichtungen der Bank aus dem Gesetz von 2004 gesammelt wurde und von der Bank nicht im Rahmen ihrer Buchhaltung verarbeitet wird, fünf Jahre nach Schließung des Kontos des Kunden gelöscht werden (es sei denn, die Bank kann nachweisen, dass für die wirksame Durchführung interner Maßnahmen zur Verhinderung oder Aufdeckung von Geldwäsche oder Terrorismusfinanzierung gemäß Artikel 3.6 des genannten Gesetzes eine verlängerte Aufbewahrungsfrist von weiteren fünf Jahren erforderlich ist).

17. Im Übrigen verpflichtet Art. 27 („Archivierung“) des Gesetzes von 2009 die Zahlungsinstitute und die E-Geld-Institute, *„gemäß den im Handelsgesetzbuch vorgesehenen Fristen alle geeigneten Aufzeichnungen aufzubewahren, damit die CSSF überprüfen kann, ob sie ihren Verpflichtungen aus diesem Gesetz nachkommen“.*

18. Darüber hinaus müssen die Kreditinstitute unter Bezugnahme auf das Gesetz vom 5. April 1993 über den Finanzsektor in seiner geänderten Fassung vorsehen, dass „jede von *ihnen erbrachte Dienstleistung, jede von ihnen ausgeübte Tätigkeit und jede von ihnen selbst vorgenommene Transaktion“ gemäß den im Handelsgesetzbuch vorgesehenen Fristen registriert und* aufbewahrt werden (Artikel 37-1 Absatz 6). Daten, die auf der Grundlage der oben genannten nationalen Bestimmungen erhoben und gespeichert werden, können daher grundsätzlich für einen Zeitraum **von höchstens 10 Jahren ab dem Ende des Geschäftsjahres, auf das sie sich beziehen, gespeichert und** anschließend vom für die Verarbeitung Verantwortlichen gelöscht oder anonymisiert werden (sofern für diese Daten keine andere längere Speicherfrist gilt).

ii. Aufbewahrungsfrist für Daten zum Zwecke der Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Gesetz 2004)

19. Gemäß Artikel 3.6 des Gesetzes von 2004, Artikel 1.5 der großherzoglichen Verordnung vom 1. Februar 2010 zur Präzisierung einiger Bestimmungen des geänderten Gesetzes vom 12. November 2004 zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung und Artikel 25 der CSSF-Verordnung Nr. 12-02 vom 14. Dezember 2012 zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung in der geänderten Fassung (im Folgenden "CSSF-Verordnung") sind die Gewerbetreibenden verpflichtet, die folgenden Dokumente, Daten und Informationen fünf Jahre nach Beendigung der Geschäftsbeziehung mit dem Kunden oder nach dem Datum der gelegentlich abgeschlossenen Transaktion aufzubewahren:
    - eine Kopie der Dokumente, Daten und Informationen, die zur Erfüllung der Sorgfaltspflichten gegenüber Kunden gemäß den Artikeln 3 bis 3-3 des Gesetzes von 2004 erforderlich sind, die Geschäftsbücher, die Geschäftskorrespondenz sowie die Ergebnisse aller durchgeführten Analysen,
    - Belege und Transaktionsaufzeichnungen, die erforderlich sind, um einzelne Transaktionen zu identifizieren oder zu rekonstruieren, um erforderlichenfalls Beweise für strafrechtliche Ermittlungen oder Ermittlungen zu liefern.

20. Die CNPD weist darauf hin, dass es sich bei den auf Vorrat gespeicherten personenbezogenen Daten z. B. um Daten handele, die in amtlichen Kundenidentifizierungsdokumenten wie Pässen, Personalausweisen, Führerscheinen oder ähnlichen Dokumenten oder Kopien dieser Dokumente enthalten seien; Untersuchungen zur Feststellung des Kontexts und des Gegenstands komplexer Transaktionen von ungewöhnlich hohem Wert; Angaben zum wirtschaftlichen Eigentümer (z. B. aus dem Register der wirtschaftlichen Eigentümer) usw.

21. Die CNPD stellt ferner fest, dass die Speicherung bestimmter Daten auf der Grundlage der oben genannten Bestimmungen in selteneren Fällen auch besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO oder personenbezogene Daten

über strafrechtliche Verurteilungen und Straftaten im Sinne von Art.[8] 10 der DSGVO betreffen kann.

22. Tatsächlich können politische Meinungen und religiöse Überzeugungen durch finanzielle Transaktionen aufgedeckt werden, zum Beispiel durch Spenden an politische Parteien oder Organisationen, Kirchen oder Pfarreien. Die Mitgliedschaft in einer Gewerkschaft kann durch die Erhebung eines Jahresbeitrags vom Bankkonto einer Person aufgedeckt werden. Personenbezogene Gesundheitsdaten können durch die Analyse von Arztrechnungen erlangt werden, die eine betroffene Person an einen Angehörigen der Gesundheitsberufe (z. B. einen Psychiater) bezahlt hat. Schließlich können Informationen über bestimmte Käufe Informationen über das Sexualleben oder die sexuelle Orientierung einer Person preisgeben.[9]

23. Im Übrigen könnten die sich aus dem Gesetz von 2004 ergebenden Sorgfaltspflichten die für die Verarbeitung Verantwortlichen dazu veranlassen, Daten über ein Gerichtsverfahren gegen eine natürliche Person zu erheben und aufzubewahren, wie die über ihre Anklageerhebung oder das Gerichtsverfahren und gegebenenfalls die sich daraus ergebende Verurteilung, die Daten über „Straftaten“ und „strafrechtliche Verurteilungen“ im Sinne von Art. 10 der DSGVO darstellen, und zwar unabhängig davon, ob in diesem Gerichtsverfahren die Begehung der Straftat, derentwegen die Person verfolgt wurde, tatsächlich festgestellt wurde oder nicht.[10]

24. Da der Kontext, in dem diese Art von Daten verarbeitet werden, erhebliche Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen mit sich bringen könnte,[11] setzen die von den Art. 9 und 10 der DSGVO erfassten Datenverarbeitungen für den Verantwortlichen eine Reihe zusätzlicher Garantien voraus, wie z. B. eine spezifische Information darüber, dass diese Datenkategorien für die Zwecke der Einhaltung des Gesetzes von 2004 verarbeitet werden können, oder einen Mechanismus, der es dem Verantwortlichen ermöglicht, sich zu vergewissern, dass die Daten aus zuverlässigen Quellen stammen, korrekt und aktuell sind.[12]

25. Unternehmen, die dem Gesetz von 2004 unterliegen, können die personenbezogenen Daten ihrer Kunden für einen zusätzlichen Zeitraum von fünf Jahren aufbewahren, „wenn *dies für die wirksame Umsetzung interner Maßnahmen zur Verhinderung oder Aufdeckung von Geldwäsche oder Terrorismusfinanzierung erforderlich ist“.* (Artikel 3.6

---

[8] Europarat, Beratender Ausschuss des Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten, Übereinkommen 108, Leitlinien zum Schutz personenbezogener Daten bei der Verarbeitung personenbezogener Daten zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (S. 20)

[9] EDSB, Leitlinien 6/2020 zum Zusammenspiel zwischen der Zweiten Zahlungsdiensterichtlinie und der DSGVO, Version 2.0, angenommen am 15. Dezember 2020 (§52); Europäischer Datenschutzbeauftragter, Stellungnahme 39/2023 zu dem Vorschlag für eine Verordnung über Zahlungsdienste im Binnenmarkt und dem Vorschlag für eine Richtlinie über Zahlungsdienste und E-Geld-Dienste im Binnenmarkt, angenommen am 22. August 2023 (Ziffer 24).

[10] Urteil vom 24. September 2019, GC u. a. (Auslistung sensibler Daten), C-136/17, EU:C:2019:773, Rn. 72.

[11] Vgl. Erwägungsgrund 51 der DSGVO.

[12] Die CNPD fordert die Verantwortlichen auf, Art. 76 der Verordnung 2024/1624 vom 31. Mai 2024 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung zur Kenntnis zu nehmen, der die in den Art. 9 und 10 DSGVO genannten Bedingungen für die Datenverarbeitung vorsieht (obwohl diese Bestimmung noch nicht anwendbar ist, könnte sie bereits als „Standard“ für die betroffenen Unternehmer dienen).

Absatz 6) oder wenn die Aufsichtsbehörden eine zusätzliche Aufbewahrungsfrist verlangen (Artikel 3.6 Absatz 5). Nach dieser Bestimmung weist die CNPD darauf hin, dass eine Dauer von zehn Jahren nicht die „Standard"-Speicherfrist für alle Kunden eines Zahlungsdienstleisters sein sollte. Es obliegt dem für die Verarbeitung Verantwortlichen, im Einklang mit dem Grundsatz der Verantwortlichkeit zu dokumentieren, warum ein zusätzlicher Zeitraum von fünf Jahren erforderlich ist.

26. Ferner ist darauf hinzuweisen, dass das Gesetz von 2004 vorsieht, dass „[u]nbeschadet *längerer Aufbewahrungsfristen, die in anderen Gesetzen vorgeschrieben sind, ... Gewerbetreibende verpflichtet [sind], personenbezogene Daten nach Ablauf der in Absatz 1 genannten Aufbewahrungsfristenzu löschen"* (Artikel 3.6 Absatz 4). Die Verpflichtung, die Daten der betroffenen Personen nach 5 oder 10 Jahren (nach Beendigung der Geschäftsbeziehung mit dem Kunden oder nach dem Zeitpunkt der gelegentlichen Transaktion) zu löschen, ergibt sich daher auch aus dem Gesetz von 2004. Daraus ergibt sich, dass die für die Verarbeitung Verantwortlichen die Daten nicht über diese Fristen hinaus für Zwecke der Bekämpfung von Geldwäsche und Terrorismusfinanzierung aufbewahren sollten.

Hervorzuheben sind: Wenn der Verantwortliche aufgrund einer rechtlichen Verpflichtung verpflichtet ist, die Daten zu löschen, darf er die zur Erfüllung dieser rechtlichen Verpflichtung erhobenen Daten nicht über die gesetzliche Aufbewahrungsfrist hinaus auf der Grundlage seines berechtigten Interesses speichern.

27. Die CNPD nimmt auch Art. 11.2 der CSSF-Verordnung in der geänderten Fassung zur Kenntnis, in dem es heißt: „Die *Kundenakzeptanzpolitik muss auch die Verfahren vorsehen, die bei einem Verdacht auf Geldwäsche, damit zusammenhängende Vortaten oder Terrorismusfinanzierung oder bei einem begründeten Verdacht auf Geldwäsche oder Terrorismusfinanzierung zu befolgen sind, wenn der Kontakt zu einem potenziellen Kunden erfolglos bleibt. Die Gründe für die Weigerung des Kunden oder des Unternehmers, eine Geschäftsbeziehung einzugehen oder eine Transaktion abzuschließen, sind nach Maßgabe des Artikels 25 dieser Verordnung zu dokumentieren und aufzubewahren, auch wenn die Weigerung des Unternehmers nicht auf die Feststellung eines Hinweises auf Geldwäsche oder Terrorismusfinanzierung zurückzuführen ist."* Folglich können die Daten einer betroffenen Person, der die Eröffnung eines Kontos verweigert wird oder die selbst auf die Eröffnung eines Kontos verzichtet, gemäß den Bestimmungen des Gesetzes von 2004 gespeichert werden.

28. Vor diesem Hintergrund unterscheidet die CNPD im Wesentlichen drei mögliche Ausgangspunkte für die Berechnung der in Art. 3.6 des Gesetzes von 2004 vorgeschriebenen Aufbewahrungsfristen:
    (i) Beendigung der Geschäftsbeziehung mit dem Kunden (z. B. Schließung des Bankkontos oder Online-Kontos einer betroffenen Person);
    (ii) das Datum eines gelegentlichen Geschäfts;
    (iii) das Datum, an dem der Kunde oder Unternehmer die Aufnahme einer Geschäftsbeziehung verweigert hat.

29. Die CNPD stellt fest, dass es vorkommen kann, dass ein Konto vom für die Verarbeitung Verantwortlichen aus Gründen der Anwendung des Gesetzes von 2004 gesperrt wird (z. B. gemäß Artikel 3.4 des Gesetzes von 2004 bis zur Überprüfung der Identität) und dass das Konto, wenn der Kunde nicht reagiert, auf unbestimmte Zeit gesperrt bleibt und keine

Speicherfrist auslöst. Da dies in bestimmten Fällen zu einer unbefristeten Speicherung der Daten der betroffenen Person unter Verstoß gegen Art. 5.1 Buchst. e der DSGVO führen kann, [13] empfiehlt die CNPD den betroffenen Verantwortlichen, einen Mechanismus einzurichten, der es ermöglicht, die betroffene Person neu zu beleben und das Konto spätestens ein Jahr nach der Sperrung des Kontos zu schließen (die personenbezogenen Daten werden in jedem Fall nach der Schließung zu Zwecken der Bekämpfung von Geldwäsche und Terrorismus aufbewahrt).

iii. Besondere Aufbewahrungsfristen für den Zweck der Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Reg. EU 2023/1113)

30. In Artikel 26.1 der Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849 wird darauf hingewiesen, dass Angaben zum Zahler und zum Zahlungsempfänger oder zum Originator und zum Begünstigten von Kryptowerten (wie unter anderem Name, Nummer des Zahlungskontos, Anschrift, Nummer des amtlichen Ausweisdokuments, Kundenidentifikationsnummer, Geburtsdatum und -ort) nicht über das unbedingt erforderliche Maß hinaus gespeichert werden. Der Zahlungsdienstleister muss diese Daten daher für einen Zeitraum von fünf Jahren aufbewahren, nach dessen Ablauf er sie löschen muss (wie in Artikel 26.2 festgelegt), es sei denn, das nationale Recht sieht etwas anderes vor, in dem festgelegt ist, unter welchen Umständen Zahlungsdienstleister die Speicherfrist für diese Daten verlängern können oder müssen. Da die personenbezogenen Daten, die von Zahlungsdienstleistern auf der Grundlage dieser Verordnung verarbeitet werden, nur zum Zwecke der Verhinderung von Geldwäsche und Terrorismusfinanzierung verarbeitet werden (Artikel 25.2), versteht die CNPD, dass der Beginn der oben genannten Aufbewahrungsfrist derselbe ist wie für die im Gesetz von 2004 vorgesehenen Verarbeitungen, d. h. die Beendigung der Geschäftsbeziehung mit dem Kunden oder das Datum der gelegentlichen Transaktion.

Beispiel 4: Eine Online-Bank verarbeitet die Nummer des amtlichen Ausweisdokuments ihres Kunden gemäß Artikel 26.1 der Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849 und den Bestimmungen des Gesetzes von 2004. Diese Daten müssen 5 Jahre nach Schließung des Kontos der betroffenen Person gelöscht werden.

iv. Aufzeichnung von Telefongesprächen und elektronischer Kommunikation

[13] Und die Anforderungen von Artikel 3.4 des Gesetzes von 2004.

31. Die Aufzeichnung von Telefongesprächen und elektronischer Kommunikation ist grundsätzlich nur unter Beachtung des geänderten Gesetzes vom 30. Mai 2005 über den Schutz der Privatsphäre im Bereich der elektronischen Kommunikation (im Folgenden: Gesetz von 2005) und der DSGVO möglich.

32. So können gemäß Art. 4.3 Buchst. d des Gesetzes von 2005 Kommunikationen aufgezeichnet werden:
    - auf der Grundlage der freiwilligen, spezifischen, in Kenntnis der Sachlage erteilten und eindeutigen vorherigen Zustimmung des Kunden; oder
    - wenn sie im Rahmen rechtmäßiger beruflicher Gepflogenheiten erfolgt, um den Nachweis eines Handelsgeschäfts oder einer anderen kommerziellen Kommunikation zu erbringen.

33. Die Ausnahme für „kommerzielle *Kommunikation"* kann sich z. B. auf Aufzeichnungen von Telefongesprächen beziehen, *die von „Callcentern",* „Helpdesks", Kundendiensten usw. geführt werden.

34. In beiden Fällen ist es erforderlich, Kunden und Mitarbeiter vorab und transparent zu informieren, insbesondere über den/die Zweck(e) der Registrierung und die Speicherdauer. Diese Information muss den Anforderungen der DSGVO entsprechen.[14]

35. Um diese Anforderungen zu erfüllen, hält es die CNPD für erforderlich, dass bei jedem überwachten Telefoninterview die Korrespondenten speziell auf die Aufzeichnung aufmerksam gemacht werden, unabhängig davon, ob zu Beginn des Anrufs eine automatisierte Nachricht gesendet wird oder nicht.

36. Was speziell die Kreditinstitute betrifft, sieht Art. 37-1 (Abs. 6bis) des Gesetzes vom 5. April 1993 über den Finanzsektor in seiner geänderten Fassung die Verpflichtung vor, *Aufzeichnungen von Telefongesprächen oder elektronischen Mitteilungen „mindestens im Zusammenhang mit Geschäften, die im Rahmen des Handels für eigene Rechnung abgeschlossen wurden, und mit der Erbringung von Dienstleistungen im Zusammenhang mit Kundenaufträgen, die den Empfang, die Übermittlung und die Ausführung von Kundenaufträgen betreffen", aufzubewahren, und zwar „fünf Jahre lang und auf Verlangen der CSSF für einen Zeitraum von bis zu sieben Jahren".*Telefongespräche und elektronische Mitteilungen müssen daher grundsätzlich fünf Jahre nach ihrer Registrierung gelöscht werden, es sei denn, eine längere Speicherung ist durch einen anderen Zweck gerechtfertigt, der mit dem ursprünglichen Zweck vereinbar ist, und eine der in Art. 6 der DSGVO vorgesehenen Zulässigkeitsgrundlagen ist anwendbar.

v. Erhebung des Personalausweises im Rahmen der Ausübung der Rechte der betroffenen Personen

[14] Siehe Artikel 12, 13 und 14 DSGVO. Weitere Informationen finden Sie auf der Website der CNPD, „Le droit à l'information", abrufbar unter https://cnpd.public.lu/de/particuliers/your-rights/droit-a-information.html.

37. Gemäß Artikel 12.6 der DSGVO kann der Verantwortliche, wenn er begründete Zweifel an der Identität der natürlichen Person hat, die den Antrag gemäß den Artikeln 15 bis 21 stellt (z. B. einen Antrag auf Auskunft oder Löschung), zusätzliche Informationen anfordern, die erforderlich sind, um die Identität der betroffenen Person zu bestätigen.

38. Generell sollte der Personalausweis nicht als geeignetes Authentifizierungsmittel zur Bestätigung der Identität der betroffenen Person angesehen werden, es sei denn, eine Verhältnismäßigkeitsprüfung belegt das Gegenteil. Eine solche Verhältnismäßigkeitsprüfung sollte die Art der verarbeiteten Daten, die Art des Antrags sowie den Kontext des Antrags berücksichtigen und gleichzeitig eine übermäßige Datenerhebung vermeiden und ein angemessenes Maß an Sicherheit bei der Verarbeitung gewährleisten[15].

39. Obwohl der Personalausweis im Allgemeinen nicht als geeignetes Authentifizierungsmittel zur Bestätigung der Identität der betroffenen Person angesehen werden sollte, kann es vorkommen, dass ein Zahlungsdienstleister eine betroffene Person, die ihre Rechte gemäß der DSGVO ausüben möchte, auffordert, eine Kopie ihres Personalausweises oder eines anderen amtlichen Dokuments zum Nachweis ihrer Identität vorzulegen (wenn eine solche Erhebung nach der DSGVO gerechtfertigt und verhältnismäßig ist). In einem solchen Fall muss der für die Verarbeitung Verantwortliche Schutzmaßnahmen ergreifen, um eine unbefugte oder unrechtmäßige Verarbeitung des Personalausweises zu verhindern. Dazu kann gehören, dass unmittelbar nach der erfolgreichen Authentifizierung der Identität der betroffenen Person keine Kopie erstellt wird, in der der Personalausweis überprüft wurde, oder dass eine Kopie eines Personalausweises gelöscht wird. Der EDSB hat im Übrigen darauf hingewiesen, dass „die spätere *Speicherung einer Kopie eines Identitätsdokuments einen Verstoß gegen die Grundsätze der Zweckbindung und der Speicherbegrenzung (Artikel 5 Absatz 1 Buchstaben b und e DSGVO) und darüber hinaus gegen die nationalen Rechtsvorschriften über die Verarbeitung der nationalen Identifikationsnummer (Artikel 87 DSGVO) darstellen kann. Der EDSA empfiehlt als bewährtes Verfahren, dass der für die Verarbeitung Verantwortliche nach Überprüfung des Personalausweises eine Notiz macht, in der beispielsweise angegeben wird, dass „der Personalausweis überprüft wurde“, um unnötiges Kopieren oder Speichern von Kopien von Personalausweisen zu vermeiden.“* [16]

40. Die CNPD weist ferner darauf hin, dass die Verarbeitung eines Personalausweises zum Zwecke der Authentifizierung im Zusammenhang mit der Ausübung der Rechte der betroffenen Personen die Verpflichtungen zur Aufbewahrung einer Kopie des Personalausweises nach dem Gesetz von 2004 unberührt lässt (die Löschung des zur Bestätigung der Identität einer Person, die beispielsweise ein Auskunftsrecht nach Art. 15 DSGVO ausübt, erhobenen Personalausweises setzt nicht voraus, dass ihr Personalausweis, der für Zwecke im Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung („AML/CFT“) aufbewahrt wird, in einer gesonderten Datenbank gelöscht wird).[17]

---

[15] EDSB, Leitlinien 01/2022 zu den Rechten betroffener Personen – Auskunftsrecht, Version 2.1, angenommen am 28. März 2023 (§70-77)
[16] EDSB, Leitlinien 01/2022 zu den Rechten betroffener Personen – Auskunftsrecht, Version 2.1, angenommen am 28. März 2023 (§79 und die dort angeführte Rechtsprechung)
[17] Siehe Punkt 2.a.iii

b. Art. 6 Abs. 1 Buchst. f der DSGVO: Erforderliche Speicherung zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen

i. Hinweis auf die Voraussetzungen für den Rückgriff auf das berechtigte Interesse

41. Art. 6.1 Buchst. f der DSGVO sieht die Rechtmäßigkeit einer Verarbeitung vor, wenn die Verarbeitung „für *die Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist, es sei denn, die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn es sich bei der betroffenen Person um ein Kind handelt".*

42. Die CNPD möchte an die drei kumulativen Voraussetzungen erinnern, unter denen sich ein Verantwortlicher auf Art. 6.1 Buchst. f der DSGVO stützen kann:[18]
    i) die Verfolgung eines berechtigten Interesses durch den für die Verarbeitung Verantwortlichen oder einen Dritten;
    ii) die Notwendigkeit der Verarbeitung personenbezogener Daten zur Verwirklichung des verfolgten berechtigten Interesses (das berechtigte Interesse an der Verarbeitung der Daten kann vernünftigerweise nicht so wirksam mit anderen Mitteln erreicht werden, die die Grundrechte und Grundfreiheiten der betroffenen Personen weniger beeinträchtigen);
    iii) Die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen nicht das berechtigte Interesse des für die Verarbeitung Verantwortlichen oder eines Dritten (z. B. wenn personenbezogene Daten unter Umständen verarbeitet werden, unter denen die betroffene Person vernünftigerweise nicht mit einer solchen Verarbeitung rechnet).

43. Die Voraussetzungen für die Anwendung des berechtigten Interesses sind eng auszulegen.[19] Das berechtigte Interesse darf keine standardmäßige Grundlage für die Rechtmäßigkeit darstellen. Die CNPD empfiehlt, für jede Verarbeitung eine Abwägung der betroffenen Rechte und Interessen vorzunehmen, die vor der betreffenden Verarbeitung detailliert und dokumentiert sein muss.

44. Dabei wird der Grad des Eingriffs in die Privatsphäre der betroffenen Personen (Verarbeitung sensibler Daten, Verarbeitung schutzbedürftiger Personen, Profiling usw.) und ihre anderen Grundrechte (Meinungsfreiheit, Informationsfreiheit, Gewissensfreiheit usw.) sowie die anderen konkreten Auswirkungen der Verarbeitung auf ihre Situation (Überwachung oder Überwachung ihrer Tätigkeiten, Ausschluss von Banken usw.)

[18] Urteil vom 4. Juli 2023, C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), Rn. 106
[19] Urteil vom 4. Juli 2023, Meta Platforms u. a. (Allgemeine Bedingungen für die Nutzung eines sozialen Netzwerks), C-252/21, ECLI:EU:C:2023:537, Rn. 92 und 93 und die dort angeführte Rechtsprechung

bewertet. Diese Auswirkungen sind zu messen, um im Einzelfall das Ausmaß des durch die Behandlung verursachten Eingriffs in das Leben der Menschen zu bestimmen.[20]

45. Der Rückgriff auf diese Rechtsgrundlage beinhaltet bestimmte zusätzliche Pflichten des für die Verarbeitung Verantwortlichen bei der Wahrnehmung der Rechte der betroffenen Personen:
    - Spezifische Informationspflicht in Bezug auf die verfolgten berechtigten Interessen (Artikel 13 Absatz 1 Buchstabe d DSGVO, wenn personenbezogene Daten bei der betroffenen Person erhoben werden, und Artikel 14 Absatz 2 Buchstabe b der DSGVO, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben wurden);
    - Widerspruchsrecht der betroffenen Person (Art. 21.1 DSGVO): das Recht der betroffenen Person, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund ihres berechtigten Interesses erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche darf die personenbezogenen Daten dann nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
    - Recht auf Einschränkung der Verarbeitung (Art. 18 der DSGVO): das Recht der betroffenen Person, die Einschränkung der Verarbeitung zu erwirken, wenn die betroffene Person gemäß Artikel 21.1 der DSGVO Widerspruch gegen die Verarbeitung eingelegt hat, während geprüft wird, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

46. Für weitere Einzelheiten zu den Kriterien, die die für die Verarbeitung Verantwortlichen erfüllen müssen, um personenbezogene Daten auf der Grundlage des berechtigten Interesses zu verarbeiten, fordert die CNPD die betroffenen Akteure auf, den Entwurf der Leitlinien des EDSB zum berechtigten[21] Interesse zur Kenntnis zu nehmen.

47. In den nächsten Abschnitten wird die CNPD die Zwecke analysieren, die auf der Grundlage des berechtigten Interesses eines Zahlungsdienstleisters verfolgt werden könnten.

ii. Speicherung von Daten, die zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind

48. In Erwägungsgrund 65 der DSGVO wird klargestellt, dass die weitere Speicherung personenbezogener Daten rechtmäßig sein sollte, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. In diesem

[20] Urteil vom 4. Juli 2023, C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), Rn. 116 und 118.
[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* (Diese Fassung der Leitlinien unterliegt der öffentlichen Konsultation).

Zusammenhang können die Verjährungsfristen daher wichtige Hinweise für die Bestimmung der Aufbewahrungsfristen geben.[22]

49. Art. 189 des Handelsgesetzbuchs bestimmt: „Verpflichtungen, *die aus Anlass ihres Handels zwischen Kaufleuten oder zwischen Kaufleuten und Nichtkaufleuten entstehen, verjähren in zehn Jahren, wenn sie keinen kürzeren Vorschriften unterliegen."* Es ist daher möglich, dass ein Zahlungsdienstleister personenbezogene Daten speichert, die er im Rahmen eines Rechtsstreits mit dem Kunden benötigt. Nur personenbezogene Daten im Zusammenhang mit der Erfüllung von Verträgen und den vom für die Verarbeitung Verantwortlichen erbrachten Dienstleistungen dürfen zu diesem Zweck gespeichert werden.

Beispiel 5: Nur die Daten, die für die Erfüllung des Vertrags zwischen einer Bank und ihrem Kunden erforderlich sind (z. B. ein Kontobeschluss), dürfen nach Schließung des Kontos der betroffenen Person aufbewahrt werden, um im Streitfall innerhalb der Verjährungsfrist von Artikel 189 des Handelsgesetzbuchs (10 Jahre) einen Beweis zu erbringen. Dagegen müssen Daten, die im Rahmen der im Gesetz von 2004 vorgesehenen Sorgfaltspflichten der Bank erhoben werden, wie Daten,*die aus „Watchlists" erhoben werden, nach 5 Jahren (in Ermangelung einer verlängerten Aufbewahrungsfrist* von 5 Jahren) gemäßArt. 3.6 Abs. 4 des Gesetzes von 2004 („Unbeschadet längerer Aufbewahrungsfristen, die in anderen Gesetzen vorgeschrieben sind, sind Gewerbetreibende verpflichtet, personenbezogene Daten nach Ablauf der in Abs.*1*genannten Aufbewahrungsfristen zu löschen") und Art. 3.6bis Abs. 2 („Die*Verarbeitung personenbezogener Daten auf der Grundlage dieses Gesetzes für andere Zwecke ist verboten")* gelöscht werden.

iii. Speicherung von Kundendaten zum Zwecke der Betrugsprävention

50. Die Betrugsprävention wird in Erwägungsgrund 47 der DSGVO als eines der möglichen berechtigten Interessen genannt, die durch Artikel 6.1 Buchstabe f der DSGVO geschützt werden.

51. Was insbesondere die Zahlungsdienstleister betrifft, ist auf die Bestimmungen von Art. 105 des Gesetzes von 2009 hinzuweisen: „Zahlungssysteme *und Zahlungsdienstleister dürfen personenbezogene Daten verarbeiten, wenn dies zurVerhütung, Ermittlung und Aufdeckung von Betrug im Zahlungsverkehr erforderlich ist.* [...]"[23].

---

[22] Stellungnahme der Nationalen Datenschutzkommission zum Gesetzentwurf Nr. 7945 zur Umsetzung der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, Beschluss Nr. 49AV25/2022 vom 21. Oktober 2022 (S. 22)

[23] Die Rechtsgrundlage für diese Art der Verarbeitung dürfte in Zukunft die gesetzliche Verpflichtung sein (Art. 6 Abs. 1 Buchst. c DSGVO): Siehe Artikel 83 des Vorschlags für eine Verordnung über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/2010. Interessanterweise heißt es in Artikel 83 des Vorschlags: „Zahlungsdienstleister *speichern die in diesem Absatz genannten Daten nicht länger, als dies für die in Absatz 1 genannten Zwecke oder nach Beendigung der Kundenbeziehung erforderlich ist."*

52. In seinen Leitlinien zur Interaktion zwischen der Zweiten Zahlungsdiensterichtlinie und der DSGVO wies der EDSB darauf hin,[24] dass die Verarbeitung personenbezogener Daten, die für die Zwecke der Betrugsprävention unbedingt erforderlich ist, ein berechtigtes Interesse des betreffenden Zahlungsdienstleisters darstellen kann, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person diese Interessen nicht überwiegen. Die Verarbeitungstätigkeiten zur Betrugsprävention sollten dann auf einer gründlichen Einzelfallbewertung durch den für die Verarbeitung Verantwortlichen im Einklang mit dem Grundsatz der Rechenschaftspflicht beruhen.

53. Darüber hinaus hat der EDSB in seinen Leitlinien zum berechtigten Interesse darauf hingewiesen, dass die Verarbeitung personenbezogener Daten im Rahmen des berechtigten Interesses an der Betrugsprävention nicht ohne Bedingungen und Einschränkungen erfolgt, insbesondere weil diese Art der Verarbeitung erhebliche Auswirkungen auf die betroffenen Personen haben kann. So heißt es beispielsweise in Erwägungsgrund 47 der DSGVO, dass die Verarbeitung personenbezogener Daten "unbedingt *erforderlich sein muss, um Betrug zu verhindern",* was in Verbindung mit dem Grundsatz der Datenminimierung gemäß Artikel 5.1 Buchstabe c der DSGVO zu sehen ist. Der EDSB weist ferner darauf hin, dass gleichzeitig der Grundsatz der Beschränkung der Speicherung gemäß Artikel 5.1 Buchstabe e der DSGVO bei der Festlegung von Strategien für die Vorratsspeicherung von Daten, die zum Zwecke der Aufdeckung oder Verhütung von Betrug verarbeitet werden, berücksichtigt werden muss.[25]

54. In der Praxis führt die Verarbeitung zu Kontroll- und Betrugsbekämpfungszwecken zu Profiling mithilfe von Algorithmen, die alle verfügbaren Daten verwenden, um eine Betrugs- oder Fehlerrisikoquote für jeden Kunden zu berechnen (z. B. auf der Grundlage einer Historie der bereits begangenen Betrugsfälle). Die CNPD erkennt die Bedeutung der Bekämpfung von Betrug im Zahlungsverkehr uneingeschränkt an, möchte jedoch daran erinnern, dass diese Algorithmen angesichts ihrer Risiken und ihrer möglichen Verzerrungen mit äußerster Vorsicht konzipiert und verwendet werden müssen.

55. Im Online-Kontext kann diese Art der Verarbeitung die Erhebung von Transaktionsdaten, aber auch von Daten im Zusammenhang mit dem Kontext eines Zahlungsvorgangs umfassen, wie z. B. Verhaltensdaten (Verhaltensanalyse wie Tastatureingabedynamik, Daten im Zusammenhang mit Kauf- und Verbrauchsgewohnheiten), Navigationsdaten und Verbindungsdaten zu Informationssystemen (Geolokalisierungsdaten, Hardwaredaten: IP-Adresse, Bildschirm- oder Browsereinstellung usw.).

56. Die Prävention, Ermittlung und Aufdeckung von Betrug im Zahlungsverkehr kann verschiedene Arten der Verarbeitung umfassen, z. B. die Aufdeckung von Handlungen, die eine Anomalie oder Unstimmigkeit aufweisen, die Verwaltung und Analyse solcher Warnungen, die Erstellung von Listen von Personen, die ordnungsgemäß als Täter von

[24] Leitlinien 6/2020 zum Zusammenspiel zwischen der Zweiten Zahlungsdiensterichtlinie und der DSGVO, Version 2.0, angenommen am 15. Dezember 2020

[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,* Rn. 104 (diese Fassung der Leitlinien ist Gegenstand einer öffentlichen Konsultation).

Handlungen identifiziert wurden, die vom für die Verarbeitung Verantwortlichen als Betrug oder Betrugsversuch eingestuft wurden. Diese Verarbeitungen können als „Profiling“ im Sinne der DSGVO bezeichnet[26] werden. Zwar kann die Vorratsspeicherung von Daten im Falle des Profilings Vorteile haben, da dem Algorithmus mehr Daten zur Verfügung stehen, doch müssen die für die Verarbeitung Verantwortlichen bei der Erhebung personenbezogener Daten den Grundsatz der Datenminimierung beachten und sicherstellen, dass sie diese personenbezogenen Daten nur so lange speichern, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich und verhältnismäßig ist.[27]

57. In Anbetracht der vorstehenden Ausführungen ist die CNPD der Ansicht, dass die Dauer der Speicherung der Daten im Rahmen der Betrugsprävention und -aufdeckung auf den Zeitraum begrenzt werden muss, der für die Erreichung dieses Zwecks unbedingt erforderlich ist. Beispielsweise erscheint die Speicherung der Daten einer betroffenen Person, bei der nach Schließung ihres Kontos während der Vertragslaufzeit kein Betrug festgestellt wurde, weder erforderlich noch verhältnismäßig. In diesem Fall ist die CNPD der Ansicht, dass der für die Verarbeitung Verantwortliche die zur Betrugsbekämpfung verarbeiteten Daten nach Beendigung des Vertragsverhältnisses mit dem Kunden löschen (oder anonymisieren) sollte.

[26] Profiling ist definiert als „jede *Form der automatisierten Verarbeitung personenbezogener Daten zur Bewertung der persönlichen Aspekte einer natürlichen Person, insbesondere zur Analyse oder Vorhersage von Aspekten der Arbeitsleistung der betroffenen Person, ihrer wirtschaftlichen Lage, ihrer Gesundheit, ihrer persönlichen Vorlieben oder Interessen, ihrer Zuverlässigkeit oder ihres Verhaltens oder ihres Standorts und ihrer Bewegungen, sofern sie Rechtswirkungen für die betreffende Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“* (Ziff. 71 der DSGVO).
[27] Vgl. Artikel-29-Datenschutzgruppe, Leitlinien für automatisierte individuelle Entscheidungsfindung und Profiling für die Zwecke der Verordnung (EU) 2016/679 (WP251rev.01, S. 13).

3. Bewährte Verfahren bei der Anwendung des Grundsatzes der Speicherbeschränkung

58. Gemäß den Artikeln 5 und 25 der DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Datenschutzgrundsätze wirksam umzusetzen und die Verarbeitung mit den erforderlichen Garantien zu versehen, um die Anforderungen der DSGVO zu erfüllen, einschließlich geeigneter technischer und organisatorischer Maßnahmen, um sicherzustellen, dass standardmäßig nur die personenbezogenen Daten verarbeitet werden, die für den jeweiligen spezifischen Zweck der Verarbeitung erforderlich sind.

a. Einrichtung eines Datensortierungsmechanismus

59. Daher muss der für die Verarbeitung Verantwortliche Maßnahmen ergreifen, die es ermöglichen, die verarbeiteten Daten nach Abschluss der Phase der laufenden Nutzung der Daten der betroffenen Person (die beispielsweise mit der Schließung des Kontos des Nutzers zusammenfällt) zu sortieren, um nur die personenbezogenen Daten zu speichern, die für die (neuen) Zwecke im Rahmen der Archivierungsphase relevant sind. Die systematische und unterschiedslose Speicherung aller Kontodaten nach Beendigung des Vertragsverhältnisses mit der betroffenen Person steht nämlich nicht im Einklang mit dem Grundsatz der Speicherbeschränkung.[28] Dieser „Löschungsmechanismus“ kann zur Löschung oder Anonymisierung personenbezogener Daten führen, die für die Zwecke der Datenspeicherung nicht erforderlich sind.

60. Der für die Verarbeitung Verantwortliche sollte daher die Speicherung der Daten in einer speziellen Archivierungsdatenbank vorsehen (a) oder zumindest eine logische Trennung in der aktiven Datenbank vorsehen (b).29
    (a) Eine physische Trennung könnte dadurch erreicht werden, dass die Daten aus dem Informationssystem extrahiert werden, um sie getrennt in einer speziellen Archivdatenbank aufzubewahren, auf die nur speziell befugte Personen zugreifen können. In diesem Fall muss die Archivierungsdatenbank über verschiedene Funktionen wie den Export, den Zugriff und die Visualisierung der gespeicherten Daten verfügen. Diese Funktionen ermöglichen es der Organisation, der betroffenen Person bei der Ausübung ihrer Rechte (Zugangsrecht usw.) zu antworten.

    (b) Bei einer logischen Trennung verbleiben die Daten in der „aktiven Datenbank“, werden aber durch eine Beschränkung der Berechtigungen eindeutig identifiziert und von den

[28] Art. 5 Abs. 1 lit. e DSGVO. Siehe Commission Nationale de l’Informatique et des Libertés, Délibération de la formation restreinte n°SAN-2024-002 du 31 janvier 2024 concernant la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS (Nationale Kommission für Informatik und Freiheiten, Beratung der beschränkten Ausbildung Nr. SAN-2024-002 vom 31. Januar 2024 über die Gesellschaft DE PARTICULIER A PARTICULIER A PARTICULIER – EDITIONS NERESSIS)

[29] Siehe Commission Nationale de l’Informatique et des Libertés (Nationale Kommission für Informatik und Freiheiten), Beschluss Nr. SAN-2022-018 vom 8. September 2022 über die GIE INFOGREFFE.

anderen Daten isoliert, um sie für Personen, die sie nicht mehr verarbeiten müssen, unzugänglich zu machen.[30]

b. Einrichtung eines Mechanismus zur Schließung „inaktiver" Konten

61. Einige Akteure bieten ihre Finanzdienstleistungen nur über die Einrichtung eines Online-Kontos an. Die CNPD stellt fest, dass diese Nutzer diese Konten häufig nicht mehr nutzen, ohne sie jedoch zu schließen, was manchmal dazu führt, dass Konten auf unbestimmte Zeit inaktiv sind, da das Fehlen einer Schließung dann verhindert, dass bestimmte Aufbewahrungsfristen in Gang gesetzt werden. Mit dem Gesetz vom 30. März 2022 über inaktive Konten, inaktive Tresore und nachrichtenlose Versicherungsverträge, das am 1. Juni 2022 in Kraft getreten ist, hat Luxemburg erstmals einen Rechtsrahmen für die Verwaltung inaktiver Konten geschaffen. Der neue Rechtsrahmen gilt für „jedes *Sichtkonto, Sparkonto, Einlagenkonto mit vereinbarter Laufzeit oder Kündigungsfrist, Wertpapierkonto, Treuhandkonto und jedes andere bei einem Institut eröffnete Konto".* Dagegen sind E-Geld-Konten im Sinne des geänderten Gesetzes vom 10. November 2009 über Zahlungsdienste vom Anwendungsbereich dieses Rechtsrahmens ausgenommen.

62. Um sicherzustellen, dass eine Verarbeitung mit den erforderlichen Garantien einhergeht, um die Anforderungen der DSGVO zu erfüllen, einschließlich des Grundsatzes der Genauigkeit und der Beschränkung der Speicherung, sollten die Verantwortlichen Maßnahmen vorsehen, um regelmäßig zu überprüfen, ob der Kontoinhaber noch die Absicht hat, das Konto online zu halten, und ob die darin gespeicherten Daten korrekt sind. Bei Konten mit einem Saldo von null empfiehlt die CNPD auch, eine Frist festzulegen, nach deren Ablauf das Konto als inaktiv gilt und (nach Unterrichtung der betroffenen Person) geschlossen werden muss. In diesem Zusammenhang hält die CNPD eine Frist von fünf Jahren für verhältnismäßig.[31]

[30] Siehe CNIL-Praxisleitfaden zu Aufbewahrungsfristen.
[31] Diese Empfehlung gilt unbeschadet der Bestimmungen des Gesetzes vom 30. März 2022 über inaktive Konten, inaktive Tresore und nachrichtenlose Versicherungsverträge.

4. Verpflichtung zur Unterrichtung der betroffenen Personen über die Speicherfristen

63. Nach Artikel 12 der DSGVO muss der Verantwortliche die betroffenen Personen bei der Kommunikation mit den betroffenen Personen „in*prägnanter, transparenter, verständlicher und leicht zugänglicher Weise in klarer und einfacher Sprache [...]*“über die vorgenommenen Verarbeitungen informieren.

a. Recht auf vorherige Unterrichtung

Gemäß Artikel 13.2 Buchstabe a (Informationen, die bereitzustellen sind, wenn personenbezogene Daten bei der betroffenen Person erhoben werden) und Artikel 14.2 Buchstabe a (Informationen, die bereitzustellen sind, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden) der DSGVO muss der Verantwortliche die betroffenen Personen über die Dauer der Speicherung der Daten (oder, wenn dies nicht möglich ist, über die Kriterien für die Festlegung dieser Dauer) informieren. Genaue Informationen über die Speicherfristen sind nämlich wichtig, um eine faire und transparente Verarbeitung zu gewährleisten, da sie dazu beitragen, dass die betroffenen Personen die Kontrolle über die Verarbeitung ihrer Daten haben.[32]

64. In Anbetracht dieser Bestimmungen erinnert die CNPD daran, dass Zahlungsdienstleister über die Aufbewahrungsfristen für personenbezogene Daten der Nutzer transparent sein müssen, insbesondere nach der Schließung ihres Kontos. Dies beinhaltet auch eine Information über die Rechtmäßigkeitsgrundlagen, die für die Speicherung ihrer Daten angewendet werden (die Bestimmung dieser Rechtmäßigkeitsgrundlagen ermöglicht es insbesondere, ihre in der DSGVO vorgesehenen Rechte zu bestimmen). In Bezug auf Artikel 6.1 Buchstabe f der DSGVO sollte die Art des berechtigten Interesses, das der Verantwortliche verfolgt, in den den betroffenen Personen zur Kenntnis gebrachten Informationen angegeben werden. Darüber hinaus wird das Transparenzgebot verstärkt, wenn es um die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne der Art.[33]9 und 10 der DSGVO geht.

b. Recht auf Auskunft bei der Ausübung der Rechte, die derzeit verarbeitet werden

[32] Siehe Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°SAN-2024-002 du 31 janvier 2024 concernant la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS (Nationale Kommission für Informatik und Freiheiten, Beratung der beschränkten Ausbildung Nr. SAN-2024-002 vom 31. Januar 2024 über die Gesellschaft DE PARTICULIER A PARTICULIER A PARTICULIER – EDITIONS NERESSIS)

[33] Footnote LDT EDPB Transparenz

65. Der Verantwortliche muss den betroffenen Personen auch klare Informationen zur Verfügung stellen, wenn diese ihre Rechte wie Auskunfts- und Löschungsrechte ausüben (Artikel 12.1 DSGVO).

66. Wendet sich eine betroffene Person im Rahmen der Ausübung ihrer DSGVO-Rechte an einen Zahlungsdienstleister und hat die betroffene Person Fragen im Zusammenhang mit der Speicherung ihrer Daten (z. B. einen Antrag auf Löschung), muss der Verantwortliche in der Lage sein, genaue Informationen zu erteilen: Speicherzwecke, Rechtmäßigkeitsgrundlagen, Ereignis, das die Speicherdauer auslöst, genaue(s) Datum(e) der Löschung, löschbare Daten und zu speichernde Daten (Informationen, die bereits im Verarbeitungsregister des Zahlungsdienstleisters enthalten sind).

Beispiel 6: Ein Nutzer (betroffene Person) beantragt die Löschung aller seiner Daten (auf der Grundlage von Artikel 17 Absatz 1 Buchstabe a der DSGVO) bei einem Zahlungsdienstleister, nachdem er seinen Vertrag mit ihm gekündigt hat. Der Zahlungsdienstleister, der als Verantwortlicher handelt, wird aufgrund der für ihn geltenden rechtlichen Verpflichtungen (Artikel 17.3 (b) DSGVO) nicht in der Lage sein, einen Großteil der Daten der betroffenen Person zu löschen. In seiner Antwort an die betroffene Person müssen die vom für die Verarbeitung Verantwortlichen bereitgestellten Informationen gemäß Artikel 12.1 der DSGVO spezifischer sein als in seiner Datenschutzerklärung und insbesondere Ausführungen zu den geltenden Rechtsvorschriften und den Datenkategorien enthalten, die nicht gelöscht werden können. Ein bloßer Verweis auf die „im Finanzsektor geltenden rechtlichen Verpflichtungen“ kann im Hinblick auf Art. 12.1 der DSGVO nicht als ausreichend angesehen werden.

Beispiel 7: Während der Archivierungsphase widerspricht ein Nutzer (betroffene Person) auf der Grundlage von Art. 21.1 der DSGVO und aus Gründen, die sich aus seiner besonderen Situation ergeben, der Verarbeitung seiner Daten auf der Grundlage des berechtigten Interesses des PSP. Nach einer etwaigen Einschränkung der Verarbeitung gemäß Artikel 18.1 Buchstabe d DSGVO muss der Verantwortliche entweder **(i)** die Daten gemäß Artikel 17.1 Buchstabe c DSGVO löschen oder **(ii)** nachweisen, dass zwingende schutzwürdige Gründe für die Verarbeitung vorliegen, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Artikel 21.1 DSGVO). In diesem Fall obliegt es dem Zahlungsdienstleister, der betroffenen Person genaue Informationen über die Verarbeitung und insbesondere über die berechtigten und zwingenden Gründe für die Verarbeitung, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, zur Verfügung zu stellen.