RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Extrait du
Bulletin Officiel des Finances Publiques-Impôts

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Identifiant juridique : BOI-TVA-DECLA-30-10-30-20260325
Date de publication : 25/03/2026

TVA - Régimes d'imposition et obligations déclaratives et comptables - Obligations d'ordre comptable - Obligation d'utilisation de logiciels ou systèmes de caisse sécurisés

Positionnement du document dans le plan :

TVA - Taxe sur la valeur ajoutée
Régimes d'imposition et Obligations déclaratives et comptables
Titre 3 : Obligations d'ordre comptable et relatives à la facturation
Chapitre 1 : Obligations d'ordre comptable
Section 3 : Obligation d'utilisation de logiciels ou systèmes de caisse sécurisés

Sommaire :

I. Champ d'application
A. Assujettis à la TVA concernés
B. Logiciels ou systèmes de caisse concernés
C. Données concernées
II. Nature des conditions à respecter
A. Condition d'inaltérabilité
B. Condition de sécurisation
C. Condition de conservation
D. Condition d'archivage
III. Modalités de justification du respect de ces conditions
A. Certificat délivré par un organisme accrédité
B. Attestation individuelle de l'éditeur du logiciel ou système de caisse
IV. Sanctions
A. En cas de production d'un faux certificat ou d'une fausse attestation individuelle
B. En cas de défaut de justification du respect de l'obligation prévue au 3° bis du I de l'article 286 du CGI

Actualité liée : 25/03/2026 : TVA - CF - Rétablissement de la possibilité de justifier du respect de l'obligation prévue au 3° bis du I de l'article 286 du CGI par la production d'une attestation individuelle délivrée par l'éditeur (loi n° 2026-103 du 19 février 2026 de finances pour 2026, art. 125)

1

En application du 3° bis du I de l'article 286 du code général des impôts (CGI), toute personne assujettie à la taxe sur la valeur ajoutée (TVA) qui effectue des livraisons de biens ou des prestations de services à destination de clients particuliers et qui enregistre les règlements reçus en contrepartie

au moyen d'un logiciel ou d'un système de caisse, est tenue d'utiliser un logiciel ou un système de caisse satisfaisant aux conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données en vue du contrôle de l'administration fiscale.

Pour plus de précisions sur la définition du logiciel ou système de caisse, il convient de se reporter au I-B § 30.

En revanche, cette disposition ne crée pas d'obligation de s'équiper d'un logiciel ou système de caisse. Le choix de l'utilisation d'un logiciel ou système de caisse appartient à chaque assujetti.

Ainsi, n'est pas soumis à cette obligation tout assujetti qui suit ses encaissements uniquement à l'aide d'un facturier ou d'un journal de caisse papier ou bien d'un logiciel de bureautique (tableur, traitement de texte, etc.) utilisé seulement pour rédiger des factures sans mémoriser les données.

Le respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données est justifié par un certificat délivré par un organisme accrédité ou par une attestation individuelle de l'éditeur.

L'administration fiscale s'assure de la détention par les assujettis contrôlés de l'attestation individuelle ou du certificat précités. Pour plus de précisions sur cette procédure, il convient de se reporter au BOI-CF-COM-20-60.

I. Champ d'application

A. Assujettis à la TVA concernés

10

Sont soumis à l'obligation prévue au 3° bis du I de l'article 286 du CGI, les assujettis à la TVA, personnes physiques ou morales, de droit privé ou de droit public, qui effectuent des livraisons de biens et des prestations de services ne donnant pas lieu à facturation conformément à l'article 289 du CGI (BOI-TVA-DECLA-30-20-30), quel que soit le secteur d'activité, dès lors qu'ils utilisent un logiciel ou système de caisse.

En conséquence, les assujettis qui réalisent l'intégralité de leur chiffre d'affaires avec un ou des professionnels sont exclus du dispositif, puisque les opérations réalisées entre professionnels uniquement (« B to B ») font obligatoirement l'objet d'une facturation.

En revanche, les assujettis qui réalisent à la fois des opérations avec des clients assujettis à la TVA (clients professionnels) et des non-assujettis (clients particuliers) relèvent du champ d'application du dispositif.

Un assujetti qui décide de délivrer des factures à un particulier, bien que la réglementation fiscale ne l'y oblige pas, demeure néanmoins tenu de respecter l'obligation de sécurisation de son logiciel ou système de caisse.

Un particulier qui réalise des ventes de biens ou prestations de services, notamment sur une plate-forme qui met en relation à distance, par voie électronique, des personnes en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un bien ou d'un service, est soumis à l'obligation de sécurisation des logiciels ou systèmes de caisse, lorsqu'il peut être qualifié d'assujetti à la TVA. Sur la qualité d'assujetti, il convient de se reporter au BOI-TVA-CHAMP-10-10-20.

Les sociétés mandatées pour la gestion des règlements des clients à l'aide de logiciels ou systèmes de caisse pour le compte d'un autre assujetti, doivent utiliser un logiciel ou un système de caisse conforme aux conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données

en vue du contrôle de l'administration fiscale.

20

Les succursales et filiales de sociétés étrangères sont dans le champ d'application de l'obligation de détenir un logiciel ou système de caisse sécurisé. Toutefois, par mesure de tempérament, les entreprises étrangères immatriculées à la TVA non établies en France sont hors champ du dispositif.

25

Conformément au 2 du II de l'article 286 du CGI, ne sont pas soumis à l'obligation d'utiliser un logiciel ou système de caisse sécurisé :

- les assujettis à la TVA bénéficiant du régime de la franchise en base mentionnée à l'article 293 B du CGI et à l'article 293 B bis du CGI ;
- les assujettis soumis au régime du remboursement forfaitaire de TVA agricole prévu à l'article 298 quater du CGI et à l'article 298 quinquies du CGI ;
- les assujettis effectuant exclusivement des opérations et prestations exonérées de TVA.

B. Logiciels ou systèmes de caisse concernés

30

Un logiciel ou système de caisse est un système informatique doté d'une fonctionnalité de caisse, laquelle consiste à mémoriser et à enregistrer extra-comptablement des paiements reçus en contrepartie d'une vente de marchandises ou de prestations de services, c'est-à-dire que le paiement enregistré ne génère pas concomitamment, automatiquement et obligatoirement la passation d'une écriture comptable.

Ne sont pas considérés comme enregistrés extra-comptablement, quel que soit le mode de paiement, les paiements pour lesquels le logiciel ou système de caisse déclenche obligatoirement, instantanément et automatiquement, sans intervention humaine, une écriture dans le système d'information comptable.

Un logiciel multi-fonctions qui, d'une part, enregistre un paiement et, d'autre part, génère un enregistrement comptable en mode « brouillard », en laissant à l'utilisateur la possibilité d'y apporter des modifications avant intégration définitive dans la comptabilité, est soumis à l'obligation de sécurisation.

Sont également visés par cette obligation tous les logiciels ou systèmes de caisse permettant l'enregistrement des règlements de leurs clients, quel que soit le mode de règlement (espèces, chèques, cartes bancaires, virements, prélèvements, etc.).

Cette obligation s'applique y compris en cas d'enregistrement sur un logiciel ou système de caisse accessible en ligne.

Sans que cette liste soit limitative, sont concernés par l'obligation les instruments de mesure réglementés, comme les balances, ainsi que les rampes de boissons automatisées, les automates de paiement, les bornes de commande autorisant des modes de règlement autre que le paiement par carte bancaire ou encore les distributeurs automatiques de marchandises (boissons, gâteaux, etc.) qui disposent d'une fonctionnalité de caisse. En revanche, les bornes de commande sans fonctionnalité de règlement ne sont pas concernées par cette obligation.

Seule doit être sécurisée la fonctionnalité de caisse ; les autres fonctions telles que celles relatives à la pesée n'ont pas à l'être.

Les instruments de mesure réglementés, munis d'un dispositif de mémorisation des règlements, qui sont utilisés à la fois pour déterminer le prix à payer des articles en fonction de la grandeur mesurée et pour enregistrer le règlement doivent être sécurisés. Il en est de même si plusieurs instruments de mesure réglementés sont interconnectés ou fonctionnent en réseau, chacun d'entre eux devant être sécurisé.

Exemple 1 : Un commerçant dispose d'une balance pour peser la marchandise qu'il vend au poids. Cette balance n'a pas de fonction de mémorisation des opérations relatives aux règlements de ses clients, elle n'a pas à être sécurisée.

Exemple 2 : Une balance, munie d'un dispositif de mémorisation des règlements, dispose donc d'une fonctionnalité de caisse, et doit être sécurisée. Il en est de même des balances connectées à un terminal point de vente ou des balances tactiles intégrées aux terminaux point de vente, qui intègrent à la fois une solution de pesage et d'encaissement.

Exemple 3 : Un commerçant qui dispose d'une balance dotée de mémorisation, enregistre les encaissements de ses clients dans une caisse enregistreuse non connectée à la balance, seule la caisse doit être sécurisée.

Exemple 4 : Un commerçant qui dispose d'une balance et qui note sur un cahier les encaissements de ses clients sans dispositif de caisse n'entre pas dans le dispositif. Ce commerçant n'a pas, par ailleurs, d'obligation de s'équiper d'un logiciel ou système de caisse.

Les terminaux de paiements seuls ou les prestataires de services de paiement, définis à l'article L. 521-1 du code monétaire et financier (CoMoFi), sont exclus du dispositif.

35

Par mesure de tempérament, est dispensé de l'obligation d'utiliser un logiciel ou système de caisse sécurisé l'assujetti qui recourt, pour tous les paiements reçus en contrepartie de toutes ses ventes ou prestations de services, à l'intermédiation directe d'un établissement de crédit régi par les dispositions du titre I^{er} du livre V du code monétaire et financier auprès duquel l'administration peut exercer son droit de communication.

Il en est de même lorsque l'assujetti recourt, pour tous les paiements reçus en contrepartie de toutes ses ventes ou prestations de services, à l'intermédiation directe d'un établissement bancaire établi au sein d'un pays de l'Union européenne soumis à l'obligation d'échange automatique d'informations en application de la directive 2011/16/UE du Conseil du 15 février 2011 modifiée relative à la coopération administrative dans le domaine fiscal et abrogeant la directive 77/799/CEE.

Cette mesure de tempérament ne s'applique pas :

- dès lors qu'une partie des ventes ou prestations est payée par un autre moyen, quelle que soit l'importance de cette partie ;
- si le prestataire de services de paiement n'a pas le statut d'établissement de crédit régi par les dispositions du titre I^{er} du livre V du code monétaire et financier auprès duquel l'administration peut exercer son droit de communication ou le statut d'établissement bancaire établi au sein d'un pays de l'Union européenne soumis à l'obligation d'échange automatique d'informations en application de la directive 2011/16/UE du Conseil du 15 février 2011 modifiée.

37

Exemple 1 : Le gérant d'un site de e-commerce qui effectue des ventes à distance de biens à des particuliers et qui n'accepte que des paiements par carte bancaire ou virement proposés par des établissements bancaires répondant aux exigences mentionnées au **I-B § 35** est dispensé, par mesure de tempérament, de l'obligation de faire sécuriser son système de caisse comme l'impose le 3° bis du I de l'article 286 du CGI, y compris lorsqu'il recourt à un prestataire de

services de paiement pour gérer ses paiements en ligne.

Exemple 2 : Le gérant d'un site de e-commerce, qui n'accepte que les moyens de paiement proposés par un prestataire de services de paiement défini à l'article L. 521-1 du CoMoFi n'est dispensé, par mesure de tempérament, de l'obligation de faire sécuriser son système de caisse, comme l'impose le 3° bis du I de l'article 286 du CGI, que si ce prestataire répond aux exigences mentionnées au **I-B § 35**.

Exemple 3 : Le commerçant qui propose, pour des achats effectués et retirés en magasin, le paiement en ligne dans la boutique (via l'application du commerçant installée sur un mobile multi-fonctions), géré par un établissement bancaire répondant aux exigences mentionnées au **I-B § 35** , mais également d'autres modes de paiement, comme les chèques cadeaux ou les espèces, ne peut se dispenser de l'obligation de sécurisation prévue au 3° bis du I de l'article 286 du CGI pour les paiements concernant ces achats.

Un mobile multi-fonctions s'entend d'un terminal mobile qui assure la téléphonie et l'accès à l'internet par voie radioélectrique, ainsi que d'autres fonctions informatiques ou multimédias.

Exemple 4 : Les automates tels que les distributeurs d'essence, les automates de péages autoroutiers ou les bornes de commandes en magasin, dès lors qu'ils ne permettent que le paiement par carte bancaire ou virement via un établissement bancaire répondant aux exigences mentionnées au **I-B § 35**, sont dispensés, par mesure de tempérament, de l'obligation de sécurisation prévue au 3° bis du I de l'article 286 du CGI.

40

Un logiciel, quelle que soit sa qualification (de caisse, comptable, de gestion ou de facturation), qui dispose d'une fonctionnalité de caisse doit satisfaire aux conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données en vue du contrôle de l'administration fiscale.

Ainsi, un logiciel de gestion qui permet de suivre les encaissements perçus en contrepartie des opérations de ventes ou de prestations de services qui concernent les non assujettis à la TVA (clients particuliers) doit être sécurisé.

De même, un logiciel de facturation, c'est-à-dire un système informatique permettant d'émettre des factures entre assujettis à la TVA, contenant les mentions obligatoires prévues à l'article 242 nonies A de l'annexe II au CGI et respectant les conditions de l'article 289 du CGI, doit être considéré comme un logiciel ou système de caisse tel que défini au **I-B § 30**, s'il dispose d'une fonctionnalité de caisse.

Ainsi, dès lors que ce type de logiciel est utilisé par un assujetti pour le suivi extra-comptable de ses règlements provenant des non assujettis, il entre dans le champ d'application du dispositif. Dans ce cas, les obligations prévues par ce dispositif s'appliquent dans les conditions de droit commun, sous réserve des spécificités prévues au **I-C § 50,** au II-C § 170 et au II-C § 190.

Dans le cas de logiciels multi-fonctions (comptabilité, gestion, caisse et facturation), seule la fonctionnalité de caisse enregistreuse et encaissement, et non l'ensemble du logiciel, doit être sécurisée.

45

Les logiciels ou systèmes de caisse dits « libres » ou développés en interne sont également concernés par l'obligation.

Un logiciel libre est un logiciel dont les utilisateurs ont un libre usage, une libre étude, une libre modification et une libre distribution. Un logiciel propriétaire, au contraire, ne permet ni légalement ni techniquement d'exercer ces quatre libertés, qui permettent aux utilisateurs d'adapter le logiciel à leurs besoins spécifiques.

Un logiciel développé en interne est un logiciel développé par l'assujetti lui-même ou par une société membre du groupe ou par un intégrateur externe.

Les modifications que les utilisateurs peuvent apporter à un logiciel libre ou développé en interne ne doivent avoir ni pour objet ni pour effet d'altérer le respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des fonctionnalités de caisse.

C. Données concernées

50

Sans préjudice d'autres dispositions spécifiques de facturation telle que l'obligation de remettre une note aux clients d'une prestation de services qui ne relèvent pas de la réglementation fiscale, les données concernées sont toutes les données liées à la réalisation d'une transaction, qu'il s'agisse d'une opération de vente d'un bien ou d'une prestation de services et qui peut conduire à l'émission, qu'elle soit antérieure, simultanée ou consécutive au règlement, d'un justificatif (note, ticket, facture, etc.) ainsi que de toutes les données liées à la réception (immédiate ou attendue) du paiement en contrepartie.

Sont ainsi visées les données de détail d'une transaction, qui doivent être enregistrées ligne par ligne, qui comprennent :

- le numéro du justificatif ;
- la date (année-mois-jour-heure-minute) ;
- le numéro de la caisse ;
- le montant total toutes taxes comprises ;
- le détail des articles ou prestations (libellé, quantité, prix unitaire, total hors taxe de la ligne, taux de TVA associé) ;
- toutes les données liées à la réception (immédiate ou attendue) du paiement en contrepartie (mode de règlement notamment) ;
- les traces de modifications et corrections apportées aux transactions enregistrées.

Est également concerné l'ensemble des données permettant d'assurer la traçabilité et de garantir l'intégrité des données concourant à la réalisation de la transaction.

Sont également concernées les données permettant de générer des données d'archive, selon un procédé fiable (II-D § 220 et suivants).

Lorsque la transaction n'est que simulée au moyen d'un module de type « école » ou « test », les données sont également concernées.

> **Remarque :** Pour les logiciels de facturation qui disposent d'une fonctionnalité de caisse, la donnée relative au numéro de caisse n'est pas exigée.

Pour plus de précisions, il convient de se reporter au BOI-BIC-DECLA-30-10-20-40 qui précise que les contribuables qui tiennent une comptabilité informatisée sont soumis aux obligations de conservation des données (livre des procédures fiscales [LPF], art. L. 102 B).

II. Nature des conditions à respecter

55

Dans les développements du présent **II § 60 à 260**, la mention « logiciel ou système de caisse » fait référence, selon le cas, aux logiciels et systèmes de caisse et, pour les logiciels multi-fonctions mentionnés au I-B § 40, à la seule fonctionnalité de caisse à sécuriser.

60

Les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données du logiciel ou du système de caisse doivent permettre à l'administration fiscale de contrôler les données enregistrées. Le logiciel ou le système de caisse doit donc prévoir un accès de l'administration fiscale à l'ensemble des données enregistrées.

Le législateur n'a pas défini de cahier des charges, ni de solution technique.

L'élaboration de référentiels ou de solutions techniques est donc du ressort des seuls acteurs privés et doit permettre le respect des quatre conditions exigées par la loi : inaltérabilité, sécurisation, conservation et archivage.

Les référentiels ou les solutions techniques évoluent en cohérence avec la loi et les instructions administratives.

70

Il est rappelé que tout logiciel ou système de comptabilité qui contient une fonctionnalité de caisse est en outre soumis aux obligations comptables, notamment au principe de l'intangibilité des écritures comptables assuré par le processus de validation des écritures (BOI-BIC-DECLA-30-10-20-40), et doit respecter, en application du I de l'article L. 47 A du LPF, les normes fixées par arrêté du ministre chargé du budget pour la remise des fichiers des écritures comptables. Pour plus de précisions, il convient de se reporter au BOI-CF-IOR-60-40.

75

Le logiciel ou le système de caisse doit enregistrer toutes les données d'origine relatives aux règlements, les rendre inaltérables, les conserver de manière sécurisée et en permettre l'archivage.

A. Condition d'inaltérabilité

80

Toutes les données mentionnées au I-C § 50 doivent être inaltérables.

90

Si des corrections sont apportées à ces données, que ce soit au moyen du logiciel ou système de caisse lui-même ou d'un dispositif externe au logiciel ou système de caisse, ces corrections (modifications ou annulations) s'effectuent par des opérations de « plus » et de « moins » et non par modification directe des données d'origine enregistrées. Ces opérations de correction donnent également lieu à un enregistrement et leur inaltérabilité doit également être garantie.

Ainsi, l'inaltérabilité des données vise à s'assurer que les données enregistrées ne peuvent pas être modifiées sans laisser de trace. Il s'agit de protéger les données non seulement contre les modifications par des tiers, ce qui constitue un délit en application de l'article 323-1 du code pénal (C. pén.), de l'article 323-2 du C. pén. et de l'article 323-3 du C. pén., mais aussi contre des modifications non tracées effectuées par le propriétaire et détenteur des données lui-même.

100

Cette inaltérabilité est garantie par :

- une inaltérabilité logique de haut niveau, en privant l'utilisateur de toute fonctionnalité du logiciel ou système de caisse lui permettant de modifier les données mentionnées au **I-C § 50**. Ce moyen

s'assortit d'une solution technique permettant de détecter et démontrer que l'utilisateur n'a pas contourné cette impossibilité fonctionnelle intégrée au logiciel ou au système de caisse de l'éditeur ;

- une inaltérabilité de bas niveau qui garantit l'intégrité des données enregistrées sur le disque sous forme de fichier ou de base de données. L'accès à une donnée par un homme de l'art ne pouvant jamais être empêché, cette inaltérabilité est garantie par la preuve que la donnée n'a pas été modifiée depuis son enregistrement (empreinte numérique à clé privée, chaînage, etc.).

Techniquement, la solution doit garantir l'inaltérabilité de toutes les données (enregistrement initial comme correction[s]) et fournir une fonctionnalité de suivi des modifications.

Ainsi, le logiciel ou le système de caisse doit prévoir que l'administration fiscale puisse accéder aux données d'origine enregistrées initialement ainsi qu'au détail daté (année-mois-jour-heure-minute) des opérations et des corrections apportées lorsque ces données ont fait l'objet de corrections.

(110)

120

Pour respecter la condition d'inaltérabilité, l'intégrité des données enregistrées doit être garantie dans le temps par tout procédé technique fiable.

La garantie d'inaltérabilité peut être obtenue par toute technique permettant :

- d'empêcher l'accès de l'utilisateur à des fonctionnalités de modification des données validées ;
- de détecter tout accès/modification des données mentionnées au **I-C § 50** et de tracer toute éventuelle modification ;
- de démontrer que ces données de règlement n'ont pas été modifiées depuis leur enregistrement initial ;
- de fournir un système de preuve en ce sens.

B. Condition de sécurisation

130

Le logiciel ou le système de caisse doit sécuriser les données mentionnées au I-C § 50, les données de modifications enregistrées et les données permettant la production des pièces justificatives émises. Il doit empêcher leur suppression ou modification sans laisser de trace.

La condition de sécurisation ne vise pas à limiter les droits d'accès au logiciel ou système de caisse mais à assurer que les enregistrements des règlements réalisés par toute personne qui accède au logiciel ou système de caisse soient mémorisés, de même que les éventuelles modifications apportées à ces enregistrements initiaux.

140

Cette sécurisation peut être assurée par tout procédé technique fiable, c'est-à-dire de nature à garantir la restitution des données dans l'état de leur enregistrement d'origine. Il peut notamment s'agir d'une technique de chaînage des enregistrements ou de signature électronique des données.

150

L'emploi d'une fonction « école » ou « test » destinée à l'enregistrement d'opérations de règlement fictives aux fins de formation du personnel doit être sécurisé, par une identification très claire des données de règlement, des pièces justificatives (par exemple en apposant la mention « factice » ou

« simulation » en trame de fond de ces documents) et de toutes les opérations enregistrées lors de l'utilisation de cette fonction, ainsi que par l'identification de l'opérateur sous la responsabilité duquel le personnel en formation enregistre les données.

C. Condition de conservation

155

La conservation des données mentionnées au I-C § 50 doit être assurée par le logiciel ou système de caisse. S'il est nécessaire de libérer de l'espace sur le disque dur ou d'améliorer la performance, ces données peuvent faire l'objet de purge, ce qui consiste à les exporter du logiciel ou système de caisse via la fonctionnalité d'archivage afin de les stocker sur un support de stockage externe au logiciel ou au système de caisse (par exemple, clé USB, disque optique, disque dur externe ou solution de stockage distant) dans les conditions prévues au II-D § 220 à 260.

L'ensemble des données doit être conservé (dans le logiciel ou système de caisse) ou archivé (sur support externe ou stockage distant). Les preuves de leur inaltérabilité et de leur traçabilité étant des données servant à l'établissement de la comptabilité de l'entreprise, elles doivent également être conservées pendant le délai de six ans prévu au premier alinéa du I de l'article L. 102 B du LPF. Elles ne nécessitent pas d'impression papier. Pour plus de précisions, il convient de se reporter au BOI-BIC-DECLA-30-10-20-40.

(160)

170

Les logiciels ou systèmes de caisse ou, s'agissant des logiciels multi-fonctions, la seule fonctionnalité de caisse, doivent prévoir obligatoirement une clôture journalière et une clôture mensuelle et annuelle (ou par exercice lorsque l'exercice ne coïncide pas avec l'année civile). Ces trois échéances sont cumulatives et impératives. Pour chaque clôture, des données cumulatives et récapitulatives, intègres et inaltérables, doivent être calculées et enregistrées par le logiciel ou système de caisse, comme le cumul du grand total de la période et le total perpétuel pour la période.

> **Remarque :** Il est admis que les logiciels de facturation qui disposent d'une fonctionnalité de caisse ne prévoient pas les clôtures journalière, mensuelle et annuelle (ou par exercice) dans leur système, sous réserve qu'en cas de contrôle ils puissent fournir, à la demande de l'administration, le total du chiffre d'affaires enregistré pour une période déterminée.

On entend par « cumul du grand total de la période » le cumul de chiffre d'affaires décompté depuis l'ouverture de la période comptable en cours.

On entend par « total perpétuel » le cumul de chiffre d'affaires décompté depuis le début de l'utilisation du logiciel ou système de caisse.

Le total perpétuel est en effet un compteur qui cumule le chiffre d'affaires total enregistré depuis le début de l'utilisation du logiciel ou système de caisse et ne se remettant jamais à zéro. Il n'est pas lié à une période contrairement au grand total qui lui est le compteur qui cumule le chiffre d'affaires total pour la période.

En cas de changement de matériel ou de logiciel, tous les compteurs repartent de zéro. Les compteurs de l'ancien matériel ou logiciel doivent être archivés et sécurisés.

Dans le cas d'un simple changement de version d'un logiciel, tous les compteurs doivent continuer à être incrémentés sans être remis à zéro.

Les totaux de contrôles produits par les procédures de clôture doivent être conservés dans le logiciel ou système de caisse et continuer d'être protégés par la garantie d'inaltérabilité. Ces données

cumulatives et récapitulatives ne doivent donc jamais être purgées. La solution logicielle doit permettre de maintenir la traçabilité des procédures d'archivage et de garantir l'inaltérabilité des données archivées.

180

Toutes les données mentionnées au **I-C § 50** doivent être conservées. Cette obligation de conservation porte sur toutes les données enregistrées ligne par ligne, et pas seulement sur le Z de caisse, ainsi que sur les données cumulatives et récapitulatives calculées par le logiciel ou système de caisse (cumul du grand total de la période et total perpétuel) (**II-C § 170**).

Un assujetti qui ne conserve que les Z de caisse ne respecte pas les obligations de conservation prévues à l'article L. 102 B du LPF. Cette définition répond à la nécessité légale de justifier les résultats produits par un système informatisé avec les données élémentaires ayant servi à leur élaboration, prises en compte dès leur origine, et non par des données agrégées résultant de traitements automatisés.

190

Lorsque l'assujetti utilise un logiciel ou système de caisse centralisé avec remontée des données mentionnées au **I-C § 50** depuis des points de vente vers un logiciel ou système centralisateur, la conservation des données sécurisées enregistrées ligne par ligne et la conservation des données cumulées peuvent être réalisées au niveau du logiciel ou système centralisateur.

200

Pour les logiciels de facturation qui disposent d'une fonctionnalité de caisse, il est admis que les données visées au **I-C § 50** soient conservées dans le module du logiciel dans lequel elles sont créées, dès lors que leur mode de conservation assure leur intégrité.

(210)

D. Condition d'archivage

220

Le logiciel ou le système de caisse doit permettre d'archiver les données enregistrées selon une périodicité choisie, au maximum annuelle ou par exercice. La procédure d'archivage a pour objet de figer les données et de donner date certaine aux données archivées.

Elle doit prévoir un dispositif technique garantissant l'intégrité dans le temps des archives produites et leur conformité aux données initiales à partir desquelles elles sont créées. Les archives peuvent être conservées dans le logiciel ou système de caisse lui-même ou en dehors du logiciel ou système de caisse lorsqu'il existe une procédure de purge.

L'obligation d'archivage ne doit pas être confondue avec une solution de sauvegarde des données présentes dans le logiciel ou système de caisse. Ces sauvegardes sont entendues comme une copie des données toujours présentes sur la caisse pour permettre la reprise technique en cas de panne de la caisse.

230

Les archives doivent pouvoir être lues aisément par l'administration en cas de contrôle, y compris lorsque l'entreprise a changé de logiciel ou de système de caisse. À cette fin, les données d'archivage doivent être enregistrées dans un format ouvert. Une notice explicative en langue française doit être jointe au contenu de l'archive.

Il est admis que les données d'archivage soient enregistrées de manière sécurisée, mais l'administration doit être en mesure de lire les données sans contrainte particulière (mise à sa disposition d'une clef de déchiffrement par l'éditeur par exemple).

240

Le logiciel ou système de caisse doit prévoir une traçabilité de la génération des données d'archives, selon un procédé fiable. Les données de traçabilité de la procédure de purge et d'archivage doivent être conservées.

250

Au-delà de la périodicité choisie et au maximum annuelle ou par exercice, le logiciel ou le système de caisse peut prévoir une procédure de purge des données. Avant la mise en œuvre d'une procédure de purge, le logiciel ou le système doit garantir la production d'un fichier d'archive complète des données mentionnées au I-C § 50, sur un support physique externe au logiciel ou système de caisse ou sur une solution de stockage distant.

Constituent notamment un support physique externe : une clé USB, un disque optique, un disque dur externe ou un serveur de stockage. Ce support physique externe doit être sécurisé. Aucune solution technique n'est imposée pour assurer cette sécurisation.

L'assujetti peut également recourir à des serveurs distants accessibles par internet ou à un tiers archiveur, qui se charge pour le compte de tiers d'assurer la conservation de ses archives.

La sécurisation du support d'archivage doit permettre de garantir l'intégrité des données archivées et leur disponibilité en cas de contrôle.

Les éditeurs doivent prévoir obligatoirement une fonction permettant de générer des fichiers d'archive pour les utilisateurs. Pour plus de sécurité, plusieurs supports de stockage différents pour une même archive peuvent être proposés. Les utilisateurs ont en effet l'obligation de conserver les données archivées pendant six ans (LPF, art. L. 102 B).

260

La décision de purger les données est liée à une contrainte (par exemple, libérer de l'espace sur le disque dur, améliorer la performance, etc.). La purge n'est que partielle : le logiciel ou système de caisse doit conserver dans un état sécurisé « en ligne », c'est-à-dire dans le logiciel ou système de caisse lui-même, les données cumulatives et récapitulatives contenues dans le grand total de la période et le total perpétuel pour la période dont les données ont été purgées.

III. Modalités de justification du respect de ces conditions

270

En application du 3° bis du I de l'article 286 du CGI, le respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données est justifié :

- soit par un certificat délivré par un organisme accrédité dans les conditions prévues à l'article L. 433-4 du code de la consommation (C. consom.) ;
- soit par une attestation individuelle de l'éditeur du logiciel ou système de caisse concerné, conforme à un modèle fixé par l'administration.

Il s'agit d'un mode de preuve alternatif : un seul de ces deux documents (certificat ou attestation individuelle) suffit à justifier du respect des conditions susvisées.

L'article 125 de la loi n° 2026-103 du 19 février 2026 de finances pour 2026 a rétabli la possibilité, à compter du 21 février 2026, de justifier du respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données d'un logiciel ou d'un système de caisse par la production d'une attestation individuelle délivrée par l'éditeur.

280

Lorsqu'une entreprise détient plusieurs logiciels ou systèmes de caisse dans lesquels elle enregistre les règlements de ses clients, elle doit présenter un certificat ou une attestation pour chacun de ces produits.

Par mesure de tempérament, dans les cas où les systèmes de caisse déployés pour l'ensemble de points de vente d'une même entité juridique sont absolument identiques en tout point, cette entité peut produire un seul certificat ou une seule attestation.

290

Qu'il s'agisse du certificat ou de l'attestation individuelle, c'est l'éditeur du logiciel ou système de caisse qui fait produire le certificat demandé à un organisme certificateur accrédité ou qui produit le document (attestation individuelle). Ce n'est pas l'assujetti qui demande la certification du logiciel ou système de caisse qu'il détient à l'autorité certifiante.

En pratique, l'éditeur remet ce document (certificat ou attestation individuelle) à l'assujetti soumis à l'obligation prévue au 3° bis du I de l'article 286 du CGI, lors de l'achat ou du téléchargement du logiciel ou système de caisse.

L'assujetti doit en effet s'assurer qu'il dispose du certificat, de sa copie ou de l'attestation individuelle correspondant à la version du logiciel ou système de caisse qu'il utilise. Par exemple s'il se procure librement et gratuitement un logiciel en ligne, il lui appartient de se faire produire une attestation individuelle ou d'obtenir une copie du certificat.

L'assujetti doit veiller à utiliser un logiciel ou système de caisse dont les fonctions afférentes aux conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage sont à jour et à disposer du certificat, de sa copie ou de l'attestation individuelle correspondant.

300

On entend par « éditeur » du logiciel ou du système de caisse la personne qui détient le code source du logiciel ou système de caisse et qui a la maîtrise de la modification des paramètres de ce produit.

Une attestation délivrée par un éditeur engage sa responsabilité sous réserve que les dispositifs techniques garantissant inaltérabilité, sécurisation, conservation et archivage ne sont pas modifiés par un tiers.

310

Lorsque le logiciel ou système de caisse est conçu de manière ouverte pour permettre son adaptation aux besoins spécifiques des clients, on entend par « éditeur » toute personne physique ou morale qui peut valablement demander la certification ou fournir l'attestation individuelle :

- soit le concepteur d'origine du logiciel ou système de caisse lorsque les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données sont respectées par le logiciel ou système de caisse conçu à l'origine par cette personne et qu'aucun des paramètres permettant le respect de ces conditions ne peut être modifié par d'autres intervenants que ce concepteur ;
- soit le dernier intervenant ayant paramétré le logiciel ou système de caisse lorsque son intervention a eu pour objet ou effet de modifier un ou des paramètres permettant le respect des conditions

d'inaltérabilité, de sécurisation, de conservation et d'archivage des données.

315

Un intervenant, quel qu'il soit, modifiant le fonctionnement du logiciel ou du système de caisse (par modification du code source, patch logiciel, paramétrage ou autre) à un point tel que les fonctionnalités techniques garantissant l'inaltérabilité, la sécurisation, la conservation ou l'archivage des données d'encaissement se trouvent modifiées, invalide le certificat ou l'attestation et se trouve soumis à l'obligation de sécurisation de la nouvelle version du logiciel ou du système de caisse.

Exemple 1 : Logiciel standard d'un éditeur fourni sous forme d'un exécutable et de ses bibliothèques logicielles non modifiables et dont le paramétrage est possible mais ne concerne pas les fonctions assurant l'inaltérabilité, la sécurisation, la conservation et l'archivage des données d'encaissement. L'éditeur de ce logiciel est soumis à une obligation de sécurisation, justifiée par un certificat délivré par un organisme accrédité ou une attestation établie par lui-même.

Exemple 2 : Logiciel hautement paramétrable, nécessitant une intégration et des développements pour être mis en service. L'éditeur fournissant le logiciel est soumis à une obligation de sécurisation, sous réserve que les développements et paramétrages de la société de service informatique procédant à l'intégration n'altèrent pas les fonctionnalités assurant l'inaltérabilité, la sécurisation, la conservation et l'archivage des données d'encaissement. Si les modifications réalisées par l'intégrateur altèrent les dispositifs techniques de sécurisation mis en place par l'éditeur, l'intégrateur devient « éditeur » (**III § 310**). Le logiciel modifié et installé doit faire l'objet d'une nouvelle procédure de sécurisation aboutissant à la délivrance d'une certification par un organisme accrédité ou d'une attestation établie par l'intégrateur « éditeur » lui-même.

Exemple 3 : Logiciel développé en interne par une entreprise. L'entreprise est considérée comme étant « l'éditeur » (**III § 310**). Elle doit faire certifier la version du logiciel en service. Toute modification du logiciel altérant les dispositifs de sécurisation des données invalide le certificat et nécessite l'établissement d'un nouveau certificat.

Exemple 4 : Logiciel libre dont le code source est fourni par la communauté de développeurs contribuant à sa programmation. Le code source permet de modifier et de recompiler à volonté le logiciel qui évolue rapidement du fait de mises à jour au fil de l'eau par la communauté de développeurs mais également de modifications en interne par l'entreprise. L'entreprise utilisatrice est donc considérée comme « l'éditeur » soumis à obligation de certification de la version actuellement en service. Toute modification par la communauté ou par l'entreprise altérant le dispositif technique de sécurisation invalide le certificat et la nouvelle version doit faire l'objet d'un nouveau certificat ou d'une nouvelle attestation.

Par mesure de tempérament, dans le cas d'une chaîne complexe d'intervenants, il est possible de faire certifier ou d'attester chaque « brique » ou module du système d'encaissement, à charge pour l'assujetti de réunir tous les documents (certificats et/ou attestations individuelles) et de pouvoir justifier que le système constitué par l'ensemble de ces « briques » ou modules est lui-même conforme aux exigences prévues au 3° bis du I de l'article 286 du CGI.

Pour cela, l'intégrateur doit recourir, en plus de la certification ou de l'attestation de chaque « brique » ou module, à une certification de services délivrée par un organisme accrédité par le comité français d'accréditation (COFRAC), instance nationale d'accréditation, dans les conditions prévues à l'article L. 433-4 du C. consom.

A. Certificat délivré par un organisme accrédité

320

Tout assujetti à la TVA soumis à l'obligation prévue au 3° bis du I de l'article 286 du CGI peut justifier que le logiciel ou système de caisse qu'il utilise pour enregistrer les règlements de ses clients satisfait à cette obligation par la production d'un certificat délivré par un organisme accrédité, dans les conditions prévues à l'article L. 433-4 du C. consom., par une instance nationale d'accréditation située en France ou dans un autre État membre de l'Union européenne, membre de la coopération européenne pour l'accréditation et ayant signé les accords de reconnaissance mutuelle multilatéraux couvrant la certification considérée.

Un éditeur dont le siège social est situé dans un État de l'Union européenne autre que la France peut donc obtenir, dans ces conditions, un certificat auprès d'un organisme accrédité dans l'État de son siège.

330

Le certificat doit explicitement mentionner que le logiciel ou le système de caisse respecte les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données prévues par la législation française au 3° bis du I de l'article 286 du CGI, telles qu'explicitées au II § 60 à 260.

Le certificat doit porter sur la version du logiciel ou système de caisse détenue par l'assujetti à la TVA ou, à défaut, sur la version majeure de ce logiciel ou système de caisse à condition, dans ce cas, que l'organisme accrédité assure un audit régulier du produit permettant de s'assurer que les versions ultérieures et non majeures de ce logiciel ou système de caisse continuent de répondre aux conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données.

Le renouvellement du certificat est fondé sur les notions d'évolutions mineures ou majeures du logiciel ou du système de caisse, et non sur une durée calendaire. Ainsi, le certificat ne doit pas nécessairement être renouvelé chaque année mais doit l'être en cas de changements majeurs apportés au logiciel ou au système de caisse.

Il est donc admis que le certificat délivré pour une version donnée d'un logiciel ou système de caisse demeure valable tant que ce dernier ne fait pas l'objet d'une nouvelle version majeure.

340

On entend par version majeure d'un logiciel ou système de caisse toute nouvelle version de ce logiciel ou système de caisse obtenue en ayant modifié, dans la précédente version de ce logiciel ou système de caisse, un ou plusieurs paramètres impactant le respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données.

À l'inverse, on entend par version mineure toute version de ce logiciel ou système de caisse obtenue sans que les paramètres impactant le respect de ces conditions aient été modifiés par rapport à la précédente version de ce logiciel ou système de caisse.

(350)

B. Attestation individuelle de l'éditeur du logiciel ou système de caisse

360

Tout assujetti à la TVA soumis à l'obligation prévue au 3° bis du I de l'article 286 du CGI peut justifier que le logiciel ou le système de caisse qu'il utilise, satisfait à cette obligation par la production d'une attestation.

365

Cette attestation est délivrée à l'assujetti, spontanément ou à sa demande, par l'éditeur du logiciel ou système de caisse au titre de la version vendue ou fournie. L'attestation peut être délivrée par un éditeur établi à l'étranger à condition d'être, soit rédigée en français, soit rédigée en langue étrangère et accompagnée d'une traduction en français certifiée.

370

L'attestation doit être individuelle, c'est-à-dire délivrée nominativement à l'assujetti à la TVA qui la produit. Une simple mention dans les conditions générales ou particulières de vente du logiciel ou système, même acceptée par l'assujetti, ne vaut pas attestation individuelle.

Toutefois, par mesure de tempérament, un document qui serait pré-rempli, sous forme papier ou dématérialisée, par l'éditeur et comportant toutes les mentions exigées, y compris la signature du représentant légal de la société éditrice, puis remis lors de l'achat physique du logiciel, sous réserve de complément par l'assujetti concernant son identification, la date d'achat et la preuve d'achat, est admis.

L'attestation doit être établie par l'éditeur du logiciel ou du système de caisse ou par son représentant légal lorsqu'il s'agit d'une société.

375

L'éditeur du logiciel ou système qui fournit l'attestation individuelle ne peut pas être l'assujetti à la TVA au nom duquel est établie l'attestation, sauf si l'activité déclarée par cet assujetti est une activité d'édition de logiciels ou de systèmes de caisse. En dehors de cette exception, lorsque le logiciel ou système est développé par l'assujetti lui-même pour ses besoins propres, ce dernier ne pourra justifier que son logiciel ou système satisfait à l'obligation prévue au 3° bis du I de l'article 286 du CGI que par la production d'un certificat délivré par un organisme accrédité dans les conditions précisées au **III-A § 320 à 340**.

L'activité d'éditeur de logiciel devra être réelle et corroborée. Les codes NAF et NACE renseignés dans les déclarations fiscales peuvent constituer une présomption simple mais ne peuvent à eux seuls être un mode de preuve de l'activité de l'assujetti et ne dispensent pas d'office de la certification par un organisme certificateur.

L'attestation doit explicitement mentionner que le logiciel ou le système de caisse respecte les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données prévues au 3° bis du I de l'article 286 du CGI, telles qu'explicitées au II § 60 à 260. Elle doit indiquer précisément le nom et les références de ce système ou de ce logiciel (y compris la version du logiciel concernée et le numéro de licence quand il en existe un) ainsi que la date à laquelle le logiciel ou système a été acquis par l'assujetti à la TVA.

380

Il sera admis que l'attestation demeure valable pour attester du respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données par les versions mineures ultérieures du logiciel ou système (sur la définition d'une version majeure et d'une version mineure, il convient de se reporter au **III-A § 340**) :

- si cette attestation identifie clairement la racine de la dernière version majeure à la date d'émission de l'attestation et les subdivisions de cette racine qui sont ou seront utilisées pour l'identification des versions mineures ultérieures ;
- et si l'éditeur s'engage à n'utiliser ces subdivisions que pour l'identification des versions mineures ultérieures, à l'exclusion de toute version majeure.

Toute nouvelle version majeure du logiciel ou système doit donner lieu à l'établissement d'une nouvelle attestation visant expressément cette version.

390

L'attestation peut être délivrée sur un support physique (par exemple, par la remise d'un document lors de l'achat du logiciel ou système à compléter par l'assujetti de son identité complète et de la date de son achat) ou de manière dématérialisée (par exemple, par téléchargement en ligne d'une attestation à compléter par l'assujetti pour y mentionner notamment son identité complète).

L'attestation doit être conforme au modèle fourni au BOI-LETTRE-000242.

IV. Sanctions

A. En cas de production d'un faux certificat ou d'une fausse attestation individuelle

400

L'établissement d'un faux document est un délit pénal passible de trois ans d'emprisonnement et de 45 000 € d'amende en application de l'article 441-1 du C. pén. Ces peines s'appliquent également aux éditeurs étrangers qui délivreraient de fausses attestations ou de fausses copies de certificat à des assujettis à la TVA en France. Elles s'appliquent aussi aux assujettis à la TVA qui présentent à l'administration une fausse copie de certificat ou une fausse attestation individuelle tout en connaissant son caractère frauduleux.

410

En cas de doute, l'administration peut s'assurer de l'authenticité du document qui lui est présenté auprès de l'organisme accrédité ou de l'éditeur qui est censé l'avoir émis.

Si cette procédure révèle que le document n'a pas été émis par l'organisme certificateur ou par l'éditeur du logiciel, l'assujetti est passible des peines applicables en cas d'établissement de faux document.

B. En cas de défaut de justification du respect de l'obligation prévue au 3° bis du I de l'article 286 du CGI

420

L'amende prévue à l'article 1770 duodecies du CGI s'applique en cas de défaut de justification du respect de l'obligation prévue au 3° bis du I de l'article 286 du CGI en matière de logiciels ou de systèmes de caisse. Pour plus de précisions, il convient de se reporter au XVIII § 550 à 580 du BOI-CF-INF-20-10-20.