ROYAUME DU MAROC

acaps

هيئة مراقبة التأمينات و الاحتياط الاجتماعي

ⵓⵍⵍⵉⵙ ⵏ ⵜⵣⴻⵎⵎⵓⵔ ⵏ ⵜⵓⵖⵍⵉⵡⵉⵏ ⴷ ⵜⵣⵔⴼⵜ ⵜⵉⵎⵓⵔⴰⵙⵜ ⵏⵜⵙⵙⵓⵔⴰⵙ

Autorité de Contrôle des Assurances et de la Prévoyance Sociale

GUIDE DE MISE EN PLACE D'UN DISPOSITIF DE VENTE EN LIGNE

SOMMAIRE

Introduction

Publiée par l'Autorité de Contrôle des Assurances et de la Prévoyance sociale (ACAPS) en juin 2022, la nouvelle instruction relative aux dispositifs électroniques de vente en ligne de produits d'assurance est entrée en vigueur le 1er juillet 2022.

Cette instruction vise à fluidifier le processus de mise en place des dispositifs de vente en ligne en fournissant aux acteurs une vision claire sur les exigences de conformité requises. Elle clarifie en effet les exigences réglementaires relatives à ce dispositif et énonce les conditions et les modalités que doivent observer les entreprises d'assurances et de réassurance ainsi que les intermédiaires d'assurances et les autres entités habilitées à présenter au public des opérations d'assurances, pour la mise en place d'un dispositif électronique de vente en ligne permettant la conclusion de contrats d'assurance.

A cet égard, il convient de souligner que la digitalisation des contrats est déjà prévue par le cadre réglementaire marocain, notamment le Dahir formant code des obligations et contrats qui stipule que « la voie électronique peut être utilisée pour mettre à disposition du public des offres contractuelles ou des informations sur des biens ou services en vue de la conclusion d'un contrat », à condition de mettre en place un processus fiable et sécurisé d'échange de consentement et de partage des éléments essentiels au contrat. Quant à la preuve du contrat, elle est traditionnellement assurée par une police d'assurance écrite et signée par les parties, processus qui peut également être digitalisé.

Il en découle que la contractualisation à distance existe dans la pratique. Dans ce cadre, la nouvelle instruction vient détailler et formaliser le processus de mise en place d'un dispositif de vente à distance de produits d'assurance.

Le présent guide passe en revue les principes liés à la formation d'un contrat d'assurance, avant de détailler le cadre légal régissant la vente en ligne (VEL), notamment les dispositions de l'instruction N° P.IN.02/2022 relative aux dispositifs dédiés à cette vente.

PARTIE 1

Contracter une assurance de manière générale, qu'est-ce que cela signifie ?

Piliers de la **contractualisation**

Un contrat valablement conclu entre deux parties possède un caractère obligatoire, lui donnant « force de loi ». Cela dit, certaines conditions doivent être respectées pour que les obligations découlant d'une déclaration de volonté soient engageantes. Il s'agit du consentement, de la capacité, d'un objet certain et enfin d'une cause licite, ou comme le stipule le DOC :

- **La capacité de s'obliger :** toute personne peut contracter si elle n'est pas déclarée incapable ;
- **Une déclaration valable de volonté portant sur les éléments essentiels de l'obligation :** le contrat est un échange de volonté, où se rencontre une offre et une acceptation. L'acceptation peut être expresse lorsque la personne exprime sa volonté par un écrit, verbalement ou bien par un simple geste ; elle est tacite lorsque la personne exprime son consentement par une attitude qui induit sa volonté de contracter. Par ailleurs, tout consentement donné par erreur, surpris par dol, ou extorqué par violence, est nul ;
- **Un objet certain pouvant former objet d'obligation :** est nulle l'obligation qui a pour objet une chose ou un fait impossible, physiquement ou en vertu de la loi.
- **Une cause licite de s'obliger :** la cause est illicite, lorsqu'elle est prohibée par la loi, ou quand elle est contraire aux bonnes mœurs ou à l'ordre public. L'obligation sans cause, ou sur une fausse cause, ou sur une cause illicite, ne peut avoir aucun effet.

Présentation des **opérations d'assurances**

La présentation des opérations d'assurances est régie par la loi n°17-99 formant code des assurances, notamment au niveau du livre quatre qui contient l'ensemble des règles à respecter par les entreprises et intermédiaires d'assurances. L'article 289 précise, ainsi, que « Les opérations pratiquées par les entreprises d'assurances et de réassurance sont présentées au public soit directement par les dites entreprises, soit par l'entremise des personnes habilitées à cet effet et dénommées «intermédiaires d'assurances».

La présentation directe des opérations d'assurances est subordonnée à l'accord préalable de l'Autorité et se fait à travers des bureaux directs de gestion, tandis qu'est intermédiaire d'assurances toute personne agréée par l'Autorité, en qualité d'agent d'assurances, personne physique ou morale, ou en qualité de société de courtage.

D'autres entités peuvent être habilitées à présenter certaines catégories d'assurances, notamment Barid Al-Maghrib et les banques pour les assurances de personnes, l'assistance et l'assurance-crédit, et les associations de micro-crédit pour les assurances de personnes et les assurances contre l'incendie et le vol, contractées par leurs clients.

Preuve du **contrat** et **Information** durant la **vie** du contrat

La loi n°17-99, en sus des règles de droit commun, régit le contrat d'assurance tant sur sa forme que sur son contenu notamment au niveau des articles 11 et 12 et encadre l'information à fournir durant la vie du contrat.

Au niveau de la forme :

- Le contrat doit **être écrit et signé par les parties**, représentant l'échange de consentement entre les parties ;
- La rédaction se fait en caractères très apparents, notamment en ce qui concerne les clauses édictant des déchéances, des cas de nullité, d'exclusion d'assurances et des cas de non-assurance ;
- Certaines clauses doivent être rappelées au-dessus de la signature, notamment celles précisant la durée du contrat.

Au niveau du contenu :

- Définition des obligations de l'assureur et de l'assuré ;
- Droit et conditions relatifs à la résiliation ;
- Droit à la restitution de la prime.
- Conditions et modalités relatives au règlement des indemnités ;
- Et autres régles prudentielles.

PARTIE 2

La vente en ligne des produits d'assurance : cadre légal

La vente à distance, telle que spécifiée précédemment est régie par une panoplie de textes de lois auxquels vient s'ajouter l'instruction n° P.IN.02/2022.

Loi n° 17-99	portant Code des Assurances
Loi n° 31-08	édictant des mesures de protection du consommateur
DOC	Le Dahir Formant Code des obligations et des contrats
Loi n° 53-05	relative à l'échange éléctronique de données jurdiques
Instruction VEL	Instruction **v**ente **e**n **l**igne

Loi n°31-08 édictant des **mesures** de **protection** du **consommateur**

Vente à distance

La loi n°31-08 édictant des mesures de protection du consommateur a consacré un chapitre à la vente à distance, qui traite du cadre régissant la fourniture à distance de biens et services et précise, au niveau de son article 27, que «Le contrat de vente à distance par un moyen électronique est valable s'il a été conclu conformément aux conditions prévues par la loi n°53-05 relative à l'échange électronique des données juridiques, et par la législation en vigueur en la matière ainsi qu'aux conditions prévues dans la présente loi».

La même loi définit les techniques de communication à distance comme tout moyen utilisé pour la conclusion d'un contrat entre un fournisseur et un consommateur sans la présence simultanée des parties et le fournisseur de service ou «cybercommerçant» comme toute personne physique ou morale utilisant, dans le cadre d'une activité professionnelle ou commerciale, le réseau Internet.

Droit d'information et rétractation

La loi n°31-08 précise par ailleurs les informations devant être comprises au niveau de l'offre de contrat et encadre l'accès du consommateur aux conditions contractuelles ainsi que leur sauvegarde.

Enfin, l'article 36 introduit le droit de rétractation du consommateur et stipule que : « Le consommateur dispose d'un délai :

- de sept jours pour exercer son droit de rétractation ;
- de trente jours pour exercer son droit de rétractation, si le fournisseur n'honore pas son engagement de confirmer par écrit les informations prévues dans les articles 29 et 32.

Et cela, sans avoir à se justifier, ni à payer de pénalités, à l'exception, le cas échéant, des frais de retour».

Lorsque le droit de rétractation est exercé, le fournisseur est tenu de rembourser, sans délai, au consommateur le montant total payé et au plus tard dans les 15 jours suivant la date à laquelle ce droit a été exercé. Au-delà, la somme due est, de plein droit, productive d'intérêts au taux légal en vigueur.

Par ailleurs, le droit de rétractation ne peut être exercé, sauf si les parties en ont convenu autrement, pour les contrats dont l'exécution a commencé, avec l'accord du consommateur, avant la fin du délai de sept jours francs.

Loi **n°53-05** relative à l'échange **électronique** de **données juridiques**

Contrats conclus sous forme électronique

L'article 3 de la loi n°53-05 relative à l'échange éléctronique de données juridiques introduit un chapitre au niveau du Dahir formant Code des obligations et des contrats qui traite des contrats conclus sous forme électronique ou transmis par voie électronique.

L'article 65-3 de ce chapitre stipule ainsi que «la voie électronique peut être utilisée pour mettre à disposition du public des offres contractuelles ou des informations sur des biens ou services en vue de la conclusion d'un contrat » tandis que l'article 65-5 précise que «pour le contrat soit valablement conclu, le destinataire de l'offre doit avoir eu la possibilité de vérifier le détail de son ordre et son prix total et de corriger d'éventuelles erreurs, et ce avant de confirmer ledit ordre pour exprimer son acceptation».

Preuve du contrat et signature

Quant à la preuve du contrat conclu à distance, l'article 417-1 du DOC précise que « l'écrit sur support électronique a la même force probante que l'écrit sur papier…. sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité».

La signature électronique, quant à elle, doit être apposée selon «un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache» et est considérée sécurisée du moment qu'elle satisfait les conditions suivantes :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure dudit acte soit détectable ;
- être produite par un dispositif de création de signature électronique attesté par un certificat de conformité.

Le certificat de conformité est délivré par **l'autorité nationale d'agrément et de surveillance de la certification électronique (la Direction Générale de la Sécurité des Systèmes d'information (DGSSI) a été désignée pour ce rôle**), lorsque le dispositif satisfait aux exigences suivantes :

- Garantir par des moyens techniques et des procédures appropriés que les données de création de la signature :
  - ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;
  - ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
  - peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.
- N'entrainer aucune altération ou modification du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

Instruction relative aux dispositifs **électroniques** de **vente en ligne** de **produits** d'**assurance**

L'instruction vente en ligne (VEL)

Elle précise que la vente en ligne des produits d'assurance est régie par :

- Les dispositions de la loi n° 17-99 portant code des Assurances ;
- Le chapitre 2 du titre IV de la loi n° 31-08 édictant des mesures de protection du consommateur ;
- Le dahir formant code des obligations et des contrats ;
- Et la loi n° 53-05 relative à l'échange éléctronique de données juridiques.

Ainsi, pour adapter les dispositions du titre IV de la loi n° 31-08 au cadre concerné, l'instruction stipule qu'il faut entendre «souscripteur» là où est mentionné le consommateur et «assureur ou distributeur» qui utilise le Dispositif, là où est mentionné le fournisseur.

PARTIE 3

Qu'est-ce qu'un dispositif de vente en ligne ?

Il s'agit de tout dispositif qui utilise le réseau Internet afin de proposer des produits d'assurance à la vente. Ce dispositif peut soit permettre la signature électronique ou la signature physique du contrat.

Toute entreprise d'assurance peut mettre en place un dispositif VEL, ainsi que tout intermédiaire d'assurance et autre entité habilitée à présenter des opérations d'assurance.

Conception du **dispositif**

Afin de mettre en place un dispositif VEL, certains éléments doivent préalablement être bien définis par l'assureur ou le distributeur, notamment :

- le choix de la cible des produits d'assurance ;
- l'étude technique de l'offre ;
- le type de dispositif choisi et le déroulement de la procédure de vente ;
- la conformité aux exigences de sécurité .

1. Choix de la cible

L'assureur ou le distributeur désirant présenter des produits d'assurance en ligne doit décider du segment sur lequel il va se positionner au niveau de son dispositif. Il s'agit d'avoir une idée claire de la clientèle ciblée et d'ajuster l'offre en conséquence, en adaptant le type de produits offerts ainsi que les modalités de souscription disponibles au niveau du dispositif.

2. Etude technique de l'offre

Un élément essentiel de tout dispositif de vente en ligne : les **conditions générales de vente,** dont la communication est obligatoire aux clients. Il s'agit d'un document visant à encadrer les relations contractuelles entre fournisseur et client, en informent ce dernier sur les conditions de vente avant toute transaction et en adaptant les différentes clauses aux particularités de leur situation. Ce document permet d'informer le client de :

- ses obligations : paiement de la prime, modalités de versement, délais de paiement, procédures de déclaration…
- ses droits : modalités et délai de rétractation…
- les obligations de l'assureur/ distributeur : information du client, disponibilité des documents, respect des délais, traitement des réclamations…

Pour ce faire, l'opérateur doit mettre en place et détailler les procédures relatives à la perception des primes, la gestion des sinistres ainsi que des réclamations, la procédure d'envoi du contrat si cela est prévu par le dispositif ainsi que les principales caractéristiques des couvertures proposées (garanties, exclusions, limites de garanties et franchise).

Concernant les modalités de gestion du contrat, des sinistres et des réclamations, l'opérateur doit prévoir un comparatif des coordonnées de la structure en charge de cette gestion avec celle du souscripteur, dans le **cas où celle-ci ne peut être faite à distance.**

Adresse du souscripteur VS Adresse de la structure de gestion du contrat : L'opérateur doit informer le souscripteur en cas de différence entre sa localité et celle de gestion des éléments relatifs à son contrat, et recueillir son accord préalablement à la conclusion du contrat.

Il est par ailleurs recommandé, concernant les intermédiaires d'assurances et autres entités agréées à présenter des opérations d'assurances, de prendre contact avec l'entreprise d'assurance dont émane les produits présentés afin de statuer sur les choix relatifs au dispositif, notamment les éléments tel que le type de dispositif choisi (de bout en bout ou avec signature manuscrite), la durée de validité de l'offre et la gestion des contrats.

3. Type de dispositif et déroulement de la procédure de vente

L'opérateur est confronté, lors de la conception de son dispositif, au choix du déroulement exact de la présentation des produits, notamment les modalités de souscription et de signature du contrat. Hormis les dispositifs se limitant à de la publicité, l'assureur/distributeur peut soit opter pour un dispositif de bout en bout, avec signature électronique, ou un dispositif avec signature manuscrite, avec ou sans conclusion en ligne.

Les différents choix sont schématisés ci-après :

Les différents types de dispositifs

Dispositif de vente en ligne

Dispositif avec signature électronique (de bout en bout)

- La contractulisation s'effectue en ligne, avec une signature électronique des deux parties (la signature peut être simple ou sécurisée);
- Le contrat doit être accessible à l'assuré à tout moment et adressé, sur sa demande, dans un délai de 7 jours.

Dispositif avec signature manuscrite (contrat physique)

Conclusion en ligne

Le contrat prend effet une fois l'assuré manifeste son consentement au niveau du Dispositif.

Le contrat physique est par la suite envoyé à ce dernier pour signature manuscrite.

Offre d'assurance

L'offre, qui doit indiquer sa durée de validité, est envoyée à l'assuré pour acceptation.

Elle ne prend effet qu'après consentement de l'assuré avant l'expiration du délai de validité.

dispostif de publicité ou devis

Dispositif qui se limite à la publicité ou à la fourniture de devis :

- doit comporter la mention : « Devis donné à titre indicatif »
- doit clarifier qu'il s'agit d'une simple publicité, au niveau de la page d'acceuil.
- l'opérateur doit communiquer à l'Autorité une fiche de présentation du dispositif au plus tard 15 jours après sa mise en service.

Signature du contrat d'assurance

Le contrat d'assurance doit être signé par les deux parties et un exemplaire est remis ou adressé au souscripteur.

Signature électronique

Lorsque le dispositif prévoit la signature électronique, il doit utiliser un procédé fiable d'identification des parties garantissant le lien de la signature électronique avec le contrat d'assurance auquel elle s'attache. Le dispositif doit ainsi permettre de garantir de manière exacte et définitive l'identité des signataires et attester que le contrat est établi et conservé d'une manière qui garantit qu'il ne peut subir aucune altération ou modification, sans faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

De plus, l'assureur ou le distributeur doit permettre au souscripteur d'accéder à son contrat électronique et d'en obtenir un exemplaire à tout moment. Il est recommandé, dans ce sens, de créer au niveau du dispositif un espace « client » accessible par ce dernier, au niveau duquel ses contrats d'assurance sont accessibles, en plus de toute autre action ou demande relative audit contrat.

Le lien entre les données de vérification de signature électronique et le signataire est attesté par un certificat électronique, qui consiste en un document établi sous forme électronique, comme le précise l'article 10 de la loi 53-05 relative à l'échange électronique de données juridiques.

Ce certificat électronique peut être simple ou sécurisé, lorsqu'il est délivré par un prestataire de services de certification électronique agréé par la DGSSI et qu'il comporte les données suivantes :

- Une mention indiquant que ce certificat est délivré à titre de certificat électronique sécurisé ;
- L'identité du prestataire de services de certification électronique et la dénomination de l'Etat dans lequel il est établi ;
- Le nom du signataire ou un pseudonyme lorsqu'il existe, celui-ci devant alors être identifié comme tel, titulaire du certificat électronique sécurisé ;
- Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat est destiné ;
- Les données qui permettent la vérification de la signature électronique sécurisée ;
- L'identification du début et de la fin de la durée de validité du certificat ;
- Le code d'identité du certificat ;
- La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat ;
- Le cas échéant, les conditions d'utilisation du certificat, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

Signature manuscrite

A défaut de la signature électronique du contrat, la signature doit être manuscrite. Dans ce cas, l'envoi au client doit préciser notamment si l'assureur ou le distributeur considère :

- Qu'il s'agit d'une offre d'assurance. Dans ce cas, l'envoi doit indiquer la durée de validité de l'offre et préciser que :
  - Le contrat ne prend naissance qu'après acceptation de l'offre par le client adressée à l'assureur ou au distributeur avant l'expiration de sa durée de validité. La signature physique du contrat par le client exprime son acceptation.
  - A défaut d'acceptation de l'offre adressée à l'assureur ou au distributeur avant l'expiration de sa durée de validité, l'offre n'est plus valable et toute somme éventuellement versée par le client lui sera restituée. Les modalités et délais de restitutions des sommes versées doivent être spécifiées au niveau du dispositif.
- Que le contrat est conclu en ligne à travers le Dispositif et qu'il est envoyé au souscripteur pour signature. La signature manuscrite vient dans ce cas postérieurement à la souscription et constitue une formalité. Le dispositif doit par ailleurs permettre l'identification des parties et garantir le lien entre le consentement de ces derniers, exprimé au niveau du dispositif, et le contrat d'assurance auquel il s'attache.

4. Conformité aux exigences de sécurité

L'opérateur doit veiller à ce que son dispositif soit mis en place dans le respect des exigences de sécurité en la matière, alignés notamment avec les guides fournis par la DGSSI.

Un questionnaire (annexe 1) est à cet effet joint à l'instruction N° P.IN.02/2022 et constitue une référence pour l'opérateur pour mettre en place une check-list lors de la conception de son dispositif, dans le but de s'assurer du respect de la réglementation et des guidelines en la matière.

Informations à communiquer à l'**ACAPS**

La mise en place d'un dispositif de vente en ligne de produits d'assurance n'est pas soumise à la validation de l'Autorité. Il incombe cela dit, à l'opérateur, préalablement à la mise en service du dispositif, d'informer l'Autorité en lui adressant les informations et les documents suivants :

- Une fiche de présentation du dispositif qui comporte :
  - L'adresse du dispositif permettant de dérouler l'ensemble des étapes du processus de souscription ;
  - Un descriptif détaillé du processus de souscription en ligne ;
  - Les conditions générales de vente ;
  - Informations relatives au respect des normes de sécurité ;
  - La liste des produits qui seront présentés ;
  - La liste des options de couverture proposées pour chaque produit ;
  - Les modalités de paiement de la prime.
- Dans le cas de signature électronique, un rapport certifiant que ce processus de signature est conforme aux exigences réglementaires. Ce rapport doit certifier également la conformité du procédé d'établissement et de conservation des contrats.
- Dans le cas de signature du contrat sous format papier, un descriptif des modalités d'envoi du contrat et de son retour signé ainsi que l'option retenue (offre d'assurance ou conclusion en ligne).

Par ailleurs, en cas de changement ou modification du dispositif déjà mis en place, l'assureur ou le distributeur doit informer l'Autorité de l'ensemble des aspects modifiés.

Il est à rappeler que, dans le cas d'un dispositif se limitant à la publicité ou à la fourniture de devis, le distributeur doit communiquer à l'Autorité une fiche de présentation du dispositif au plus tard 15 jours après sa mise en service.

Informations à fournir au niveau du **dispositif**

1. La page d'accueil du dispositif doit contenir :

- Les « conditions générales de vente » de manière permettant leur conservation et reproduction. Lesdites conditions doivent être acceptées par le client, avant toute souscription et être disponibles à tout moment à ce dernier d'une manière qui permet de les conserver à son niveau ou de les reproduire.
- Les informations relatives à l'EAR, l'intermédiaire, ou l'entité habilitée à présenter les produits d'assurance (dénomination, adresse du siège social, numéro et date de l'agrément…) ;
- Le Dispositif non utilisé directement par un assureur doit indiquer pour chaque produit la dénomination de l'assureur dont il émane.

2. Le dispositif contient **les éléments relatifs à l'offre** de manière claire et compréhensible :

- L'identification des principales caractéristiques des couvertures proposées, notamment les garanties assorties des exclusions, les limites de garantie, les modalités de paiement des primes et, éventuellement, les franchises et les plafonds d'indemnisation ;
- Le nom ou la dénomination sociale de l'assureur ou du distributeur, les coordonnées téléphoniques qui permettent de communiquer effectivement avec lui, son adresse et, s'il s'agit d'une personne morale, son siège social ;
- L'indication de l'adresse de l'assureur ou des assureurs qui prennent en charge les garanties du produit lorsqu'il s'agit d'un dispositif utilisé par un distributeur ;
- L'existence, le cas échéant, du droit de rétractation prévu à l'article 36 de la loi n° 31-08 susvisée ;
- La durée de validité de l'offre et la prime y afférente ;
- Le cas échéant, le coût de l'utilisation du dispositif électronique supporté par le souscripteur ;
- Le cas échéant, la durée minimale du contrat proposé.

3. Le dispositif doit **communiquer, avant la souscription** et par voie électronique :

- La confirmation des informations mentionnées dans l'encadré ci-dessus, à moins que l'assureur ou le distributeur n'ait satisfait à cette obligation au préalable ;
- Les modalités de gestion du contrat et des sinistres éventuels y afférents ainsi que les coordonnées de la

structure en charge de cette gestion. Ces modalités doivent notamment préciser le mode de gestion (physique, digital ou hybride) ;

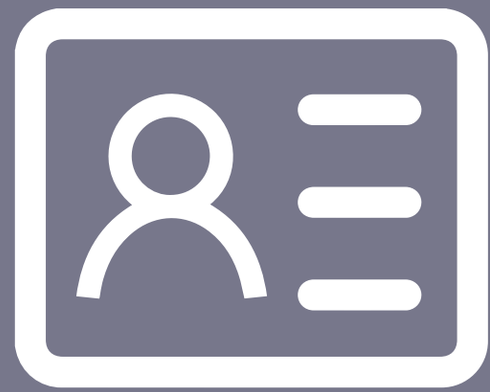
- Les modalités d'examen des réclamations éventuelles au sujet du contrat ainsi que les coordonnées de la structure où ces réclamations peuvent être présentées (adresse, numéro de téléphone) ;
- Les conditions et les modalités d'exercice du droit de rétractation prévu à l'article 36 de la loi n° 31-08 ainsi qu'un modèle de lettre destiné à faciliter l'exercice de ce droit ;
- Les conditions de résiliation du contrat lorsque le contrat est d'une durée supérieure à un an.

4. Le Dispositif doit **rappeler les choix du souscripteur** avant la conclusion et lui permettre de confirmer ou modifier sa demande.

L'assureur ou le distributeur ne peut stipuler que sa responsabilité est exclue ou limitée à l'égard du client en ce qui concerne le bon fonctionnement ou la fiabilité du Dispositif ou l'exactitude des renseignements qui y sont présentés.

PARTIE 4

Lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)



Rappel des **exigences** relatives à l'**identification**, la **vérification** de l'**identité** et la connaissance de la **clientèle** dans le cadre de la **LBC/FT**

Les articles 13, 14, 15, 16 et 33 de la circulaire LBC/FT édictent les mesures à mettre en place par les personnes assujetties en termes :

- d'identification ;
- de vérification d'identité ;
- de connaissance des clients ;
- des informations et documents à collecter; et ce en fonction de l'appréciation du risque de chaque relation d'affaires.

Ainsi, dès l'entrée en relation avec un prospect, l'entreprise ou l'intermédiaire d'assurance est tenu d'appliquer des mesures d'identification, et ce quel que soit le profil de risque du prospect.

Ensuite, le professionnel de l'assurance doit être en mesure de vérifier l'identité du client. Cette exigence est obligatoire avant l'entrée en relation, pour la vigilance standard et peut être opérée après l'entrée en relation pour la vigilance simplifiée. Cette vérification est faite sur la base de documents d'identités probants, valides et authentiques.

Le professionnel peut également étendre le périmètre de connaissance du client, à travers le recueil de toute information supplémentaire permettant la connaissance du client et l'identification, le cas échéant, de tout bénéficiaire effectif.

Si le client ou l'opération présente un risque élevé, le professionnel adopte des mesures de vigilance renforcée.

Il est entendu que les informations recueillies doivent être régulièrement tenues à jour et que les exigences de vigilance s'appliquent également aux clients en portefeuille.

Exigences relatives à la **LBC/FT** dans le cadre de la **vente en ligne** de **produits** d'**assurance**

L'entrée en relation à distance pose certaines difficultés pour opérer une identification et une vérification de l'identité qui soit équivalente à celle effectuée lors de l'entrée en relation avec présence physique du client. Ainsi, la personne assujettie est tenue de mettre en place des mesures de vigilance permettant d'assurer une certaine « équivalence au face à face». Dans ce sens, la personne assujettie doit être dotée de :

- Systèmes, équipements et logiciels fiables et sécurisés permettant l'identification et la vérification de l'identité du client et la fiabilité des moyens d'identification de manière à établir le lien entre les documents d'identité et ledit client ;
- Moyens de contrôle permettant la gestion et l'atténuation des risques de fraude liés à l'usage des technologies précitées.

Que faire en cas d'**absence** ou d'**insuffisance** de moyens permettant d'**assurer** une «**équivalence** au face à face » ?

En l'absence des moyens prévus au premier point du paragraphe précédent ou lorsque ces moyens ne satisfont pas aux conditions qui y sont requises, les personnes assujetties sont tenues d'appliquer, selon une approche basée sur les risques, les mesures de vigilance supplémentaires appropriées permettant l'atténuation des risques, notamment :

- Demander une pièce supplémentaire permettant de s'assurer de l'identité du client ;
- Appliquer une ou plusieurs mesures de vigilance.

Par ailleurs, il est à signaler que dans le cadre de l'application de l'approche basée sur les risques susmentionnée, et particulièrement des mesures de vigilances simplifiées prévues au niveau de l'article 19 de la circulaire LBC/FT, les personnes assujetties peuvent s'abstenir de la mise en place des moyens électroniques visant la vérification à distance de l'identité des clients et bénéficiaire dans le cas des opérations et personnes citées au niveau dudit article, à condition d'exiger la présentation des documents d'identité physiques (documents originaux); et ce au plus tard au moment de la prestation.

Annexe : Questionnaire relatif au respect des exigences de la sécurité

Abrégés : O : Oui, **N** : Non, **P :** Partiellement

VOLET REFERENTIELS – NORMES - ORGANISATION	O	N	P	COMMENTAIRE
• Alignement avec la loi n°09-08 pour les traitements liés au processus de vente en ligne (*)	☐	☐	☐	
• L'authenticité du contrat est-elle assurée par des moyens robustes ?	☐	☐	☐	
• Certification du circuit de paiement PCI-DSS	☐	☐	☐	
• Alignement avec les guides de la DGSSI	☐	☐	☐	
« Guide de sécurité des applications Web » :				
• Phase avant-projet (nommée CPS)	☐	☐	☐	
• Développement de l'application	☐	☐	☐	
• Production de l'application	☐	☐	☐	
« Guide relatif à l'externalisation » :				
• Hébergement sur le territoire national	☐	☐	☐	
• Hébergement dédié	☐	☐	☐	
• Plan Assurance Sécurité établi	☐	☐	☐	
• Réversibilité assurée	☐	☐	☐	
« Guide de gestion des risques » :				
• Application classée comme un « actif »	☐	☐	☐	
• Les risques liés sont-ils appréciés et traités ?	☐	☐	☐	
• Les mesures sont-elles définies pour les risques de l'application ?	☐	☐	☐	

« Guide PCA / PRA » (**) :

- Couverture de l'application par le plan de secours informatique ☐ ☐ ☐
- Si oui, est ce que ce plan est testé régulièrement ? ☐ ☐ ☐
- Une durée maximale d'interruption de service acceptable est-elle définie pour le processus de l'application ? ☐ ☐ ☐
- Perte tolérée de données est-elle définie pour le processus de l'application ? ☐ ☐ ☐
- Respect et adoption des normes et référentiels de bonnes pratiques
  - Respect et certification CMMI (***) du maitre d'œuvre ☐ ☐ ☐
  - OWASP (****) ☐ ☐ ☐
  - ISO 27001 ☐ ☐ ☐
  - Autres normes / référentiels à indiquer : .....
- Obligation de confidentialité pour les intervenants internes et externes
  - Chartes utilisateurs / administrateurs ☐ ☐ ☐
  - Clauses de confidentialité prestataires : Maitre d'œuvre Projet, Tierce Maintenance Applicative (TMA) ☐ ☐ ☐

VOLET TECHNIQUE – SECURITE ET QUALITE DU SYSTEME

- Audit périodique (Architecture, Configurations, codes sources…)

  - Fréquence de l'audit interne

    ☐ Trimestrielle
    ☐ Semestrielle
    ☐ Annuelle
    ☐ Bi annuelle

  - Fréquence de l'audit externe

    ☐ Trimestrielle
    ☐ Semestrielle
    ☐ Annuelle
    ☐ Bi annuelle

- Tests d'intrusion

  - Fréquence

    ☐ Trimestrielle
    ☐ Semestrielle
    ☐ Annuelle
    ☐ Bi annuelle

  - Types (*****)

    ☐ Boite Blanche
    ☐ Boite Grise
    ☐ Boite Noires

- Gestion des vulnérabilités et des mises à jour
  - Réalisation de scans de vulnérabilités ? ☐ Oui ☐ Non
  - Mises à jour déployées pour corriger les vulnérabilités identifiées ? ☐ Oui ☐ Non

- Dispositifs de sécurité

Pare-feu

- Multiniveaux (E-O, N-S) ☐ Oui ☐ Non
- Haute Disponibilité (HA) ☐ Oui ☐ Non
- Fonctionnalités UTM ☐ Oui ☐ Non

Mécanismes d'identification des clients

- Utilisation d'une authentification à double facteur ☐ Oui ☐ Non
- Outils KYC (Know Your Customer) : scan CNIE, selfies, etc. ☐ Oui ☐ Non

Autres, à préciser : .....

Firewall Applicatif intégrant les modules :

- Anti-attaque « XSS » et « injections SQL » ☐ Oui ☐ Non
- Anti-attaque « Brute Force » ☐ Oui ☐ Non

Autres, à préciser : .....

Autre mécanismes anti « Brute Force » :

- Rate Limiting ☐ Oui ☐ Non
- Capatcha ☐ Oui ☐ Non
- Mots de passe forts ☐ Oui ☐ Non

Autres, à préciser : .....

Autres dispositifs

- Chiffrement SSL ☐ Oui ☐ Non
- Antivirus / Antiransomware ☐ Oui ☐ Non

Autres, à préciser : .....

Processus de veille de sécurité et application

- Notifications Macert ☐ Oui ☐ Non
- Autre source (ex : MITRE, Editeurs, CERT privées, etc.) : .....

Supervision de sécurité / Journal des incidents de sécurité

- Enregistrement de toutes les activités d'authentification et de changement de droits ☐ Oui ☐ Non
- Logs centralisés dans un serveur protégé en accès et modification ☐ Oui ☐ Non
- Supervision SOC/SIEM, avec des use cases définies ☐ Oui ☐ Non
- Traitement à part des incidents de sécurité ☐ Oui ☐ Non

(*) : les autorisations de la CNDP dans le cas de la collecte des numéros de CNIE, ou des données à caractère personnelles exploitées à d'autres fins autres que celles pour lesquelles elles ont été collectées, ou dans le cas de transfert des données à l'étranger.

(**) Plan de Continuité des activités (PCA) : Programme d'entreprise, qui engage celle-ci dans la durée, et dont l'objectif est de limiter les impacts financiers, stratégiques, juridiques et d'images liés aux risques d'arrêt d'une activité essentielle de l'organisation. Il définit un ensemble de mesures visant à assurer, en fonction de différents scénarios de crise, y compris en cas de survenance de risques majeurs, le maintien de sa capacité à répondre à ses missions et le maintien des prestations de services essentielles, puis la reprise progressive de toutes les missions et les activités réalisées.

PRA : Document structuré, présentant la démarche à suivre en cas de survenance d'un sinistre imprévu. Il permet à l'entité concernée d'adopter les meilleures dispositions afin de minimiser les effets dudit sinistre sur son activité et d'assurer, le plus rapidement possible, un retour vers un fonctionnement normal de ses fonctions critiques.

(***) Capability Maturity Model Integratio (CMMI) : un cadre méthodologique qui vise l'amélioration des processus de gestion de projet de développement et permet de mesurer la maturité d'une organisation et son efficacité sur une échelle de 1 à 5.

(****) OWASP : organisation internationale à but non lucratif qui se consacre à la sécurité des applications web. Elle publie régulièrement un rapport « Top 10 » qui détaille les 10 risques les plus critiques.

(*****) Boite Noire : sans posséder la moindre information sur la cible. L'objectif est donc ici de déterminer la vulnérabilité d'un système face aux attaques d'un hacker externe.

(*****) Boite Grise : tenter de s'introduire dans un système d'information en ne disposant que d'un nombre limité d'informations sur l'organisation ou son système

(*****) Boite Blanche : le pentester a accès à la totalité des informations sur le système. On simule donc l'intrusion d'une personne ayant un accès avec un rôle applicatif.

Adresse : Avenue Al Araar, Hay Riad, Rabat - Maroc
Tél : +212 (5) 38 06 08 18
Fax : +212 (5) 38 06 08 99 / 08 01
E-mail : contact@acaps.ma
Site web : www.acaps.ma