ROYAUME DU MAROC

acaps

Autorité de Contrôle des Assurances et de la Prévoyance Sociale

Rabal, le 08 JUIN 2022

P.IN.02/2022

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

Le Président par intérim de l'Autorité,

Vu la loi n° 17-99 portant code des assurances promulguée par le dahir n° 1-02-238 du 25 rajeb 1423 (3 octobre 2002) telle qu'elle a été modifiée et complétée ;

Vu la loi n° 64-12 portant création de l'Autorité de contrôle des assurances et de la prévoyance sociale promulguée par le dahir n° 1-14-10 du 4 joumada I 1435 (6 mars 2014), notamment son article 19,

Décide

La présente instruction a pour objet d'énoncer les conditions et modalités que doivent observer les entreprises d'assurances et de réassurance désignées ci-après « assureur(s) » ainsi que les intermédiaires d'assurances et les autres entités habilitées à présenter au public des opérations d'assurances, désignés ci-après « Distributeur(s) », qui souhaitent mettre en place un dispositif électronique de vente en ligne permettant la conclusion de contrats d'assurance.

Dans ce cadre, cette instruction reprend, notamment, les principales règles portant sur les contrats conclus à distance prévues par 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 électronique de données juridiques ainsi que certaines dispositions de la loi n° 17-99 portant code des assurances et des textes pris pour son application applicables à la vente en ligne.

Section I : Définitions et champs d'application

Article 1 :

On entend par dispositif électronique de vente en ligne de produits d'assurance, désigné ci-après « Dispositif », tout dispositif qui utilise le réseau internet pour proposer à la vente des produits d'assurance, que ce dispositif permette ou non la signature électronique des contrats d'assurance.

ACAPS BO

Ne peuvent utiliser des Dispositifs que les assureurs et les Distributeurs.

N'est pas considéré comme Dispositif, le dispositif électronique qui se limite à la publicité ou à la fourniture de devis à titre indicatif. Dans ce dernier cas, le devis doit comporter la mention : « Devis donné à titre indicatif ».

Le dispositif électronique se limitant à la publicité, régi par les dispositions de la loi n° 31-08 précitée applicables aux publicités, doit mentionner de manière claire sur la page d'accueil qu'il s'agit d'une simple publicité ne comportant aucun engagement de l'utilisateur.

Les dispositions prévues aux 1er, 2ème et 4ème alinéas de l'article 10 et au 2ème alinéa de l'article 11 de la présente instruction ne sont pas applicables aux Dispositifs s'adressant exclusivement à des personnes physiques ou morales pour la souscription de contrats d'assurance en vue de la satisfaction de leurs besoins professionnels.

Article 2 :

La vente en ligne des produits d'assurance est régie notamment par les dispositions de la loi n° 17-99 précitée, du chapitre 2 du titre IV de la loi n° 31-08 susvisée, du dahir formant code des obligations et des contrats et de la loi n° 53-05 précitée.

Pour l'application dudit chapitre 2 du titre IV de la loi n° 31-08 précitée, il y a lieu d'entendre :

- le souscripteur là où est mentionné le consommateur ;
- l'assureur ou le Distributeur qui utilise le Dispositif, là où est mentionné le fournisseur.

Article 3 :

L'assureur ou le Distributeur qui utilise le Dispositif doit mettre en place toutes les mesures nécessaires pour satisfaire aux exigences législatives et réglementaires applicables.

Article 4 :

L'assureur doit s'assurer, dans le cadre de son système de contrôle interne, de la conformité de son Dispositif aux exigences législatives et réglementaires applicables et celles de la présente instruction.

Section II : Conditions et modalités applicables aux dispositifs électroniques de vente en ligne des produits d'assurance

Sous-section I : Règles applicables aux dispositifs électroniques de vente en ligne des produits d'assurance

Article 5 :

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.

Article 6 :

Lorsqu'un assureur utilise un Dispositif, la présentation de l'opération d'assurance à travers ce Dispositif est effectuée directement par l'assureur conformément aux dispositions de l'article 289 de la loi n° 17-99 précitée à travers un ou plusieurs bureaux de gestion directe.

Dans ce cas, les coordonnées (adresse, adresse mail et numéro de téléphone) du bureau de gestion directe doivent figurer dans les conditions particulières du contrat.

Dans le cas où le dispositif électronique d'un assureur oriente des clients vers le Dispositif d'un Distributeur en vue de la souscription du contrat, la présentation doit être effectuée entièrement par ce Dispositif.

Article 7 :

Lorsque l'adresse du souscripteur/assuré est située dans une localité différente de celle de la structure où il peut présenter et suivre ses demandes relatives à la gestion du contrat et des sinistres et ses réclamations, le Dispositif doit signaler cette différence et recueillir, préalablement à la conclusion du contrat, la confirmation du souscripteur.

Les dispositions du présent article ne sont pas applicables lorsque lesdites opérations peuvent être faites par un dispositif électronique.

Sous-section II : Information préalable des souscripteurs de contrats d'assurance à travers le Dispositif

Article 8 :

Le Dispositif doit permettre au souscripteur d'accéder facilement aux conditions contractuelles applicables à la fourniture de produits d'assurance à distance désignées « Conditions générales de vente » et d'en prendre connaissance sur la page d'accueil.

Ces conditions doivent être mises à la disposition du souscripteur d'une manière permettant leur conservation et leur reproduction.

Article 9 :

La page d'accueil du Dispositif utilisé par un assureur doit indiquer la dénomination de l'entreprise d'assurances suivie, en caractères uniformes et apparents, de la mention "Entreprise régie par la loi n° 17-99 portant code des assurances", sa forme juridique, le montant de son capital social ou, le cas échéant, de son fonds d'établissement, l'adresse de son siège social et son numéro d'inscription au registre du commerce.

Pour le Dispositif utilisé par un intermédiaire d'assurances, la page d'accueil doit indiquer le nom ou la dénomination sociale de l'intermédiaire d'assurances suivi(e) de la mention "Intermédiaire d'assurances régi par la loi n° 17-99 portant code des assurances" ainsi que le numéro et la date de son agrément.

Pour le Dispositif utilisé par une autre entité habilitée à présenter les opérations d'assurance, la page d'accueil doit préciser la dénomination de l'entité, le numéro et la date de son agrément/autorisation ainsi que l'adresse de son siège social.

En sus, les Dispositifs visés aux deux alinéas précédents doivent indiquer pour chaque produit présenté, la dénomination de l'assureur ou des assureurs qui prennent en charge les garanties du produit.

Article 10 :

Toute offre de contrat d'assurance par le moyen d'un Dispositif doit comporter les informations suivantes :

- 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.

Ces informations doivent être communiquées au souscripteur, avant la conclusion du contrat, de manière claire et compréhensible par tout moyen adapté au Dispositif utilisé.

L'offre de contrat d'assurance par voie électronique doit comporter en sus :

- Les différentes étapes à suivre pour conclure le contrat par voie électronique et, notamment, les modalités selon lesquelles les parties se libèrent de leurs obligations réciproques ;
- Les langues proposées pour la conclusion du contrat ;
- Les modalités d'archivage du contrat par l'assureur ou le Distributeur et les conditions d'accès au contrat archivé ;
- Les moyens techniques permettant au souscripteur, avant la conclusion du contrat, d'identifier les erreurs commises dans la saisie des données et de les corriger.

En outre, le Dispositif doit, avant la conclusion du contrat, rappeler au souscripteur ses différents choix et lui permettre de confirmer sa demande ou de la modifier selon sa volonté et ce, sans préjudice des dispositions de la loi n° 53-05 précitée.

Article 11 :

Préalablement à la souscription du contrat, un exemplaire du projet de contrat comportant le prix ou la notice d'information prévue à l'article 10 de la loi n° 17-99 précitée qui décrit notamment les garanties assorties des exclusions, le prix y afférent et les obligations de l'assuré doit être remis par voie électronique au souscripteur.

En outre, avant la conclusion du contrat, le souscripteur doit recevoir, par voie électronique :

- La confirmation des informations mentionnées au 1er alinéa de l'article 10 de la présente, 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 susvisée 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.

Article 12 :

Les informations nécessaires pour la conclusion du contrat d'assurance peuvent être :

- Soit transmises par courrier électronique par le souscripteur s'il a accepté expressément l'usage de ce moyen. Cette acceptation n'est pas requise pour le souscripteur professionnel qui a communiqué son adresse électronique ;

- Soit recueillies au moyen d'un formulaire transmis par voie électronique aux souscripteurs ou mis à la disposition de ces derniers via le Dispositif.

Sous-section III : Exigences spécifiques à la lutte contre le blanchiment de capitaux

Article 13 :

Les assureurs et Distributeurs qui entendent présenter des opérations d'assurance ou faire souscrire des contrats d'assurance à travers un Dispositif, doivent se conformer aux dispositions législatives et réglementaires applicables en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, notamment celles de la circulaire du Président de l'Autorité de contrôle des assurances et de la prévoyance sociale n° AS/02/19 du 25 septembre 2019 relative aux obligations de vigilance et de veille interne incombant aux entreprises d'assurances et de réassurance et aux intermédiaires en matière d'assurances et de réassurance telle qu'elle a été modifiée et complétée.

Section III : Signature et conclusion du contrat

Article 14 :

Le contrat d'assurance doit être signé par les deux parties conformément à la réglementation en vigueur. Un exemplaire du contrat dûment signé est remis ou adressé au souscripteur.

Lorsque le contrat d'assurance n'est pas conclu, toute somme éventuellement versée par le souscripteur doit lui être restituée.

Article 15 :

Lorsque le Dispositif prévoit la signature électronique du contrat, 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. Dans ce cas, la signature électronique du contrat exprime le consentement du souscripteur.

Le contrat doit être établi et conservé dans des conditions à en assurer l'intégrité.

L'assureur ou le Distributeur doit permettre au souscripteur d'accéder à tout moment à son contrat électronique et d'en obtenir un exemplaire ou doit le lui adresser à sa demande dans un délai de 7 jours à compter de la réception de cette demande.

Article 16 :

A défaut de 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 :

a) 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 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.

Ou

b) Que le contrat est conclu en ligne à travers le Dispositif et qu'il est envoyé au souscripteur pour signature.

L'assureur ou le Distributeur doit s'assurer de la cohérence entre le processus prévu par le Dispositif et l'option retenue parmi celles visées aux a) et b) ci-dessus.

Pour le Dispositif utilisé par un Distributeur, ce dernier doit fixer l'option à retenir parmi celles visées aux a) et b) précitées, y compris la durée de validité de l'offre, en commun accord avec l'assureur ou les assureurs qui prennent en charge les garanties du contrat.

Section IV : Procédure relative au contrôle du dispositif électronique de vente en ligne

Article 17 :

Préalablement à la mise en service du Dispositif, l'assureur ou le Distributeur adresse à l'Autorité :

1. Une fiche de présentation du Dispositif. Cette fiche comporte notamment :
   - L'adresse du Dispositif ;
   - Un descriptif détaillé du processus de souscription en ligne, y compris le processus d'identification, de connaissance de la clientèle et de l'exercice de vigilance au sens de la circulaire relative au devoir de vigilance ;
   - Les conditions générales de vente ;
   - Un questionnaire, selon le modèle joint à la présente, dûment renseigné sur le respect des normes de sécurité par le Dispositif ;
   - La liste des produits qui seront présentés à travers le Dispositif ;
   - La liste des options de couverture proposées pour chaque produit ;
   - Les modalités de paiement de la prime.

2. Dans le cas de signature électronique, un rapport dûment motivé et validé par les représentants légaux de l'assureur ou du Distributeur ou les personnes déléguées par eux à cet effet certifiant que ce processus de signature est conforme aux exigences réglementaires applicables en la matière. Ce rapport doit certifier également que le procédé d'établissement et de conservation des contrats est conforme aux conditions prévues à l'article 15 ci-dessus.
3. 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 parmi celles visées au a) et b) de l'article 16 ci-dessus.

L'assureur ou le Distributeur doit permettre à l'Autorité d'accéder au projet de Dispositif et de dérouler l'ensemble des étapes du processus de souscription.

En cas de changement dans le Dispositif, les dispositions concernées du présent article s'appliquent aux aspects modifiés.

Article 18 :

Pour les dispositifs qui se limitent à la publicité ou à la fourniture de devis à titre indicatif, l'assureur ou le Distributeur est tenu de communiquer à l'Autorité une fiche de présentation de son dispositif et ce, au plus tard 15 jours suivant leur mise en service.

En cas de changement dans le dispositif, les dispositions de l'alinéa précédent s'appliquent aux aspects modifiés.

Article 19 :

La présente instruction entre en vigueur le 1er juillet 2022.

Les assureurs et Distributeurs doivent se mettre en conformité avec ses dispositions à compter de cette date.

Autorité de Contrôle des Assurances et de la Prévoyance Sociale
ACAPS
BO

Président par intérim
Othman Khalil ELALAMY

ROYAUME DU MAROC

acaps

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 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 » :				
o Phase avant-projet (nommée CPS)	☐	☐	☐	
o Développement de l'application	☐	☐	☐	
o Production de l'application	☐	☐	☐	
« Guide relatif à l'externalisation » :				
o Hébergement sur le territoire national	☐	☐	☐	
o Hébergement dédié	☐	☐	☐	
o Plan Assurance Sécurité établi	☐	☐	☐	
o Réversibilité assurée	☐	☐	☐	
« Guide de gestion des risques » :				
o Application classée comme un « actif » ?	☐	☐	☐	
o Les risques liés sont-ils appréciés et traités ?	☐	☐	☐	
o Les mesures sont-elles définies pour les risques de l'application ?	☐	☐	☐	

« Guide PCA / PRA » (**) :			
o Couverture de l'application par le plan de secours informatique	☐	☐	☐
o Si oui, est ce que ce plan est testé régulièrement ?	☐	☐	☐
o Une durée maximale d'interruption de service acceptable est-elle définie pour le processus de l'application ?	☐	☐	☐
o Perte tolérée de données est-elle définie pour le processus de l'application ?	☐	☐	☐
■ Respect et adoption des normes et référentiels de bonnes pratiques			
o Respect et certification CMMI (***) du maitre d'œuvre	☐	☐	☐
o OWASP (****)	☐	☐	☐
o ISO 27001	☐	☐	☐
o Autres normes / référentiels à indiquer :			
■ Obligation de confidentialité pour les intervenants internes et externes			
o Chartes utilisateurs / administrateurs	☐	☐	☐
o 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…)	
o Fréquence de l'audit interne	☐ Trimestrielle
	☐ Semestrielle
	☐ Annuelle
	☐ Bi annuelle

o Fréquence de l'audit externe	☐ Trimestrielle	
	☐ Semestrielle	
	☐ Annuelle	
	☐ Bi annuelle	
■ Tests d'intrusion		
o Fréquence	☐ Trimestrielle	
	☐ Semestrielle	
	☐ Annuelle	
	☐ Bi annuelle	
o Types (*****)	☐ Boite Blanche	
	☐ Boite Grise	
	☐ Boite Noires	
■ Gestion des vulnérabilités et des mises à jour		
o Réalisation de scans de vulnérabilités ?	☐ Oui ☐ Non	
o Mises à jour déployées pour corriger les vulnérabilités identifiées ?	☐ Oui ☐ Non	
■ Dispositifs de sécurité		
Pare-feu		
o Multiniveaux (E-O, N-S)	☐ Oui ☐ Non	
o Haute Disponibilité (HA)	☐ Oui ☐ Non	
o Fonctionnalités UTM	☐ Oui ☐ Non	

Mécanismes d'identification des clients	
o Utilisation d'une authentification à double facteur	☐ Oui ☐ Non
o Outils KYC (Know Your Customer) : scan CNIE, selfies, etc.	☐ Oui ☐ Non
Autres, à préciser :	
Firewall Applicatif intégrant les modules :	
o Anti-attaque « XSS » et « injections SQL »	☐ Oui ☐ Non
o Anti-attaque « Brute Force »	☐ Oui ☐ Non
Autres, à préciser :	
Autre mécanismes anti « Brute Force » :	
o Rate Limiting	☐ Oui ☐ Non
o Capatcha	☐ Oui ☐ Non
o Mots de passe forts	☐ Oui ☐ Non
Autres, à préciser :	
Autres dispositifs	
o Chiffrement SSL	☐ Oui ☐ Non
o Antivirus / Antiransomware	☐ Oui ☐ Non
Autres, à préciser :	

■ Processus de veille de sécurité et application		
o Notifications Macert	☐ Oui ☐ Non	
o Autre source (ex : MITRE, Editeurs, CERT privées, etc.) :		
■ Supervision de sécurité / Journal des incidents de sécurité		
o Enregistrement de toutes les activités d'authentification et de changement de droits	☐ Oui ☐ Non	
o Logs centralisés dans un serveur protégé en accès et modification	☐ Oui ☐ Non	
o Supervision SOC/SIEM, avec des use cases définies	☐ Oui ☐ Non	
o 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 définir 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.*