JORF n°0113 du 18 mai 2010

Texte n°29

ARRETE

Arrêté du 17 mai 2010 portant approbation du cahier des charges applicable aux opérateurs de jeux en ligne

NOR: BCRB1012617A

Le ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, la ministre de la santé et des sports, le ministre du budget, des comptes publics et de la réforme de l'Etat, le ministre de l'alimentation, de l'agriculture et de la pêche et la secrétaire d'Etat chargée des sports,

Vu la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ;

Vu la délibération du collège de l'Autorité de régulation des jeux en ligne en date du 17 mai 2010,

Arrêtent :

Article 1

Le cahier des charges applicable aux opérateurs de jeux en ligne, adopté par la délibération du collège de l'Autorité de régulation des jeux en ligne en date du 17 mai 2010 et annexé au présent arrêté, est approuvé.

Article 2

Le présent arrêté et son annexe seront publiés au Journal officiel de la République française.

Annexe

A N N E X E

CAHIER DES CHARGES

Préambule

Il est rappelé que, conformément à l'article 1er de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne (la Loi), les jeux d'argent et de hasard font l'objet d'un encadrement strict au regard des enjeux d'ordre public, de sécurité publique et de protection de la santé et des mineurs ;

Qu'en outre, en vertu de l'article 3 de la Loi, la politique de l'Etat en matière de jeux d'argent et de hasard a pour objectif de limiter et d'encadrer l'offre et la consommation des jeux et d'en contrôler l'exploitation afin de :

1° Prévenir le jeu excessif ou pathologique et protéger les mineurs ;

2° Assurer l'intégrité, la fiabilité et la transparence des opérations de jeu ;

3° Prévenir les activités frauduleuses ou criminelles ainsi que le blanchiment de capitaux et le financement du terrorisme ;

4° Veiller au développement équilibré et équitable des différents types de jeu afin d'éviter toute déstabilisation économique des filières concernées ;

Qu'il résulte de l'article 34-II de la Loi que l'Autorité de régulation des jeux en ligne (ARJEL) instruit les dossiers de demande d'agrément des opérateurs de jeux ou de paris en ligne et délivre les agréments en veillant au respect des objectifs de la politique des jeux d'argent et de hasard mentionnés à l'article 3 de la Loi ;

Que, selon l'article 21 de la Loi, l'agrément ou son renouvellement est notamment conditionné à la démonstration par l'entreprise de sa capacité technique, économique et financière à faire face durablement aux obligations attachées à son activité, à la sauvegarde de l'ordre public, de la lutte contre le blanchiment des capitaux et le financement du terrorisme, des nécessités de la sécurité publique et de la lutte contre le jeu excessif ou pathologique.

Dispositions générales

La demande d'agrément

2.1.1. Toute entreprise sollicitant l'agrément prévu à l'article 21 de la Loi en tant qu'opérateur doit présenter une demande d'agrément par catégorie de jeux ou de paris (paris hippiques en ligne, paris sportifs en ligne, jeux de cercle en ligne).

2.1.2. Le renouvellement de l'agrément est soumis aux mêmes conditions et aux mêmes modalités que la demande d'agrément initiale. Il est rappelé en conséquence à l'opérateur souhaitant solliciter le renouvellement de son agrément qu'il doit prendre en considération les délais d'instruction de sa demande et dès lors qu'il convient de déposer une demande de renouvellement d'agrément dans des délais suffisants compte tenu de la date d'expiration de l'agrément.

Retrait et dépôt du dossier de demande d'agrément

2.2.1. L'agrément prévu à l'article 21 de la Loi est subordonné au dépôt auprès de l'ARJEL d'un dossier de demande d'agrément comprenant les éléments précisés dans le corps du présent texte. L'entreprise sollicitant un agrément doit utiliser les formulaires mis à la disposition des candidats par l'ARJEL.

Le dossier de demande d'agrément doit soit être retiré auprès de l'ARJEL, 99-101, rue Leblanc, 75015 Paris, aux jours et heures d'ouverture, soit être téléchargé à partir du site de l'ARJEL à l'adresse www.arjel.fr.

2.2.2. Le dossier de demande d'agrément est signé par le ou les demandeurs s'il s'agit d'une entreprise non constituée sous la forme d'une personne morale ou, s'il s'agit d'une personne morale, par le représentant légal tel que désigné par les statuts ou une personne spécialement habilitée justifiant d'un pouvoir.

2.2.3. Le dossier de demande d'agrément est déposé à l'ARJEL aux jours et heures d'ouverture ou envoyé par lettre avec accusé de réception à l'attention du président de l'ARJEL à l'adresse suivante : 99-101, rue Leblanc, 75015 Paris.

2.2.4. Le dossier de demande d'agrément est rédigé en langue française. Les pièces et documents fournis à l'appui de la demande d'agrément sont rédigés ou traduits en français. Dans le cas où l'ARJEL estime que la traduction fournie n'est pas satisfaisante ou en cas de doute sur sa sincérité, elle demande une traduction établie par un traducteur assermenté.

Les documents versés au dossier de demande d'agrément peuvent être produits en copie. En cas de doute sur la conformité des copies à l'original, l'ARJEL est fondée à solliciter la présentation de ce dernier. La procédure d'instruction est suspendue jusqu'à la production de cet original.

2.2.5. Un dossier de demande d'agrément comprend :

— le formulaire de demande d'agrément ;

— les formulaires de tableaux financiers ;

— le formulaire de vérification des pièces ;

— l'ensemble des pièces à fournir ;

— le formulaire d'engagement de donner accès aux représentants de l'ARJEL au frontal conformément à l'article 16 de la Loi.

Le dossier de demande d'agrément est établi et fourni en un (1) exemplaire sous format papier souple, fort, lisse, blanc, mat et durable, de format A4. Chaque feuille est utilisée dans son sens vertical ou horizontal et sa lecture s'opère de gauche à droite. Les feuilles sont numérotées consécutivement en chiffres arabes. L'entreprise établit et fournit, en outre, deux exemplaires supplémentaires du formulaire de demande d'agrément et des formulaires de tableaux financiers.

Le dossier de demande d'agrément est également communiqué sous format PDF, sur DVD ou CD, en cinq (5) exemplaires (hors codes sources). Les codes sources sont chiffrés et exclusivement délivrés sur deux DVD ou CD, à part.

Pour la version papier du dossier de demande d'agrément, les parties juridiques et financières, d'une part (parties 3 à 10 incluse du cahier des charges), et la partie technique du dossier de demande d'agrément, d'autre part (partie 11 du cahier des charges), devront être physiquement séparées.

La partie juridique et financière devra comporter les huit sous-parties suivantes, non reliées entre elles, comprenant pour chacune les pièces à fournir correspondantes et identifiées selon la nomenclature suivante :

« Informations personnelles » : partie 3 du cahier des charges.

« Informations économiques, financières et comptables » : partie 4 du cahier des charges.

« Informations relatives au site de jeux en ligne » : partie 5 du cahier des charges.

« Informations relatives aux opérations de jeux ou de paris en ligne proposées » : partie 6 du cahier des charges.

« Informations relatives aux comptes joueurs » : partie 7 du cahier des charges.

« Informations relatives à la lutte contre les activités frauduleuses ou criminelles, en particulier le blanchiment de capitaux et le financement du terrorisme » : partie 8 du cahier des charges.

« Informations relatives à la lutte contre le jeu excessif ou pathologique » : partie 9 du cahier des charges.

« Prévention des conflits d'intérêts » : partie 10 du cahier des charges.

La partie technique devra comporter les quatre sous-parties suivantes, non reliées entre elles, comprenant pour chacune les pièces à fournir correspondantes et identifiées selon la nomenclature suivante :

« Frontal » : partie 11.2 du cahier des charges.

« Logiciel de jeu » : partie 11.3.1 du cahier des charges.

« Plate-forme de jeu » : partie 11.3.2 du cahier des charges.

« Maturité sécurité des systèmes d'information (SSI) » : parties 11.4 et 11.5 du cahier des charges.

Au sein de la partie « Logiciel de jeu », trois documents devront être présentés séparément :

— le rapport d'analyse de vulnérabilités ;

— le rapport d'analyse du générateur de nombre aléatoire, le cas échéant ;

— le rapport d'analyse de la conformité aux règles du jeu.

Pour la version électronique du dossier de demande d'agrément, les parties juridiques et financières, d'une part (parties 3 à 10 incluse du présent cahier des charges), et la partie technique du dossier de demande d'agrément, d'autre part (partie 11 du présent cahier des charges), devront également être fournies sur des supports distincts.

La version électronique de la partie juridique et financière devra comporter dans un répertoire les huit sous-répertoires suivants :

« Informations personnelles » : partie 3 du cahier des charges.

« Informations économiques, financières et comptables » : partie 4 du cahier des charges.

« Informations relatives au site de jeux en ligne » : partie 5 du cahier des charges.

« Informations relatives aux opérations de jeux ou de paris en ligne proposées » : partie 6 du cahier des charges.

« Informations relatives aux comptes joueurs » : partie 7 du cahier des charges.

« Informations relatives à la lutte contre les activités frauduleuses ou criminelles, en particulier le blanchiment de capitaux et le financement du terrorisme » : partie 8 du cahier des charges.

« Informations relatives à la lutte contre le jeu excessif ou pathologique » : partie 9 du cahier des charges.

« Prévention des conflits d'intérêts » : partie 10 du cahier des charges.

La version électronique de la partie technique (hors codes sources) devra comporter dans un répertoire les quatre sous-répertoires suivants, consacrés à la partie systèmes d'information :

« Frontal » : partie 11.2 du cahier des charges.

« Logiciel de jeu » : partie 11.3.1 du cahier des charges.

« Plate-forme de jeu » : partie 11.3.2 du cahier des charges.

« Maturité sécurité des systèmes d'information (SSI) » : parties 11.4 et 11.5 du cahier des charges.

Au sein de la partie « Logiciel de jeu », trois fichiers ou répertoires devront être présentés séparément :

— le rapport d'analyse de vulnérabilités ;

— le rapport d'analyse du générateur de nombres aléatoires, le cas échéant ;

— le rapport d'analyse de la conformité aux règles du jeu.

Les codes sources seront chiffrés et fournis sur deux supports DVD ou CD qui leur seront uniquement dédiés.

2.2.6. Si l'entreprise a son siège social établi en dehors de France, elle communique les équivalents des pièces exigées au présent cahier des charges.

Phase préparatoire à l'instruction

2.3.1. A réception du dossier de demande d'agrément, l'ARJEL procède à son enregistrement et en accuse réception.

2.3.2. L'ARJEL ouvre les dossiers de demande d'agrément et vérifie qu'ils comportent l'ensemble des pièces et des éléments d'informations prévus au cahier des charges. Lorsque le dossier de demande est incomplet, l'ARJEL adresse au candidat un courrier lui demandant d'y remédier dans un délai qui ne peut être inférieur à quinze jours. L'instruction est suspendue pendant ce délai. Si, à l'expiration du délai imparti, les informations ou pièces demandées ne sont pas parvenues à l'ARJEL, la demande d'agrément est rejetée.

Instruction de la demande d'agrément

Au cours de l'instruction, l'entreprise candidate est tenue de fournir, à la requête de l'ARJEL, toute information de nature à éclairer cette dernière sur des pièces ou des éléments contenus dans le dossier déposé.

Le collège se prononcera sur la demande d'agrément dans un délai qui ne peut être supérieur à quatre mois à compter du dépôt de la demande d'agrément, sauf les cas de suspension ou de prolongation de délai prévus au présent cahier des charges.

Modification des éléments constitutifs de la demande

Toute modification d'un élément du dossier de demande d'agrément intervenue pendant l'instruction de ce dernier est immédiatement communiquée à l'ARJEL. Elle fait courir un nouveau

délai d'instruction de quatre (4) mois.

Modalités de paiement des droits mentionnés

à l'article 1012 du code général des impôts

En application de l'article 1012 du code général des impôts, un droit fixe est dû par chaque opérateur pour toute demande de délivrance d'un agrément ou de renouvellement de celui-ci. Le montant de ce droit varie en fonction du nombre d'agréments (paris hippiques, paris sportifs, jeu de cercle) dont la délivrance ou le renouvellement est sollicité par un même opérateur. Le montant de ce droit est fixé par décret.

Le paiement est acquitté :

— pour les entreprises établies en France (ou établies dans la Communauté européenne mais ayant désigné en France, avant le 1er janvier 2002, un représentant mentionné à l'article 289 A du code général des impôts) auprès soit du service des impôts des entreprises (SIE) compétent au regard de leur lieu d'établissement (ou le lieu d'imposition de ce représentant), soit, si leur situation le justifie, auprès de la direction des grandes entreprises (DGE) ;

— pour les entreprises établies dans un autre Etat membre de la Communauté européenne auprès de la recette de la direction des résidents à l'étranger et des services généraux (DRESG) ;

— pour les autres entreprises, auprès du service des impôts des entreprises dont dépend le lieu d'imposition du représentant désigné en application de l'article 289 A du code général des impôts ou, à défaut, de l'article 302 bis ZN du même code.

Le paiement du droit fixe intervient dans un délai de trente jours à compter de la réception du dossier de demande d'agrément par l'ARJEL. L'opérateur justifie par tous moyens auprès de l'ARJEL du paiement de ce droit.

Informations personnelles

Si l'entreprise n'est pas une personne morale

Elle justifie :

a) **De l'identité de son ou de ses propriétaires qu'il s'agisse de personnes physiques ou de personnes morales, par la production d'une copie d'une pièce d'identité pour les premières, d'un extrait K bis ou un équivalent pour les secondes** et, le cas échéant, du contrat de société en participation ;

b) De son numéro SIRET ou un équivalent, et de ceux de ses associés s'il s'agit d'une société en participation ;

c) De l'adresse de son ou de ses propriétaires par la fourniture d'un justificatif de domicile et, s'il s'agit d'une société en participation, par la fourniture de documents attestant du siège social de ses associés ou de leur domicile. L'entreprise produit également les statuts des personnes morales associées, s'il s'agit d'une société en participation ;

d) De son adresse (du lieu de son ou ses établissements où l'activité est exercée, du domicile personnel du ou des propriétaires), de la localisation de ses équipements et, s'il s'agit d'une société en participation, du lieu du siège social de ses associés, de celui de leurs filiales et de celui des sociétés détenant le contrôle desdits associés.

A cet effet, elle communique à l'ARJEL ses déclarations fiscales, celles de ses associés et des filiales de ceux-ci s'il s'agit d'une société en participation.

Elle informe l'ARJEL :

a) Du ou des noms commerciaux utilisés pour son activité.

b) Des condamnations, devenues définitives, dont elle-même, son ou ses propriétaires ont, le cas échéant, fait l'objet depuis moins de dix ans, comme auteur ou complice :

Par une juridiction française, pour tout crime ou pour les délits dont la liste suit :

1° Infractions prévues au livre II de la première partie du code pénal :

— trafic de stupéfiants, prévu par la section IV du chapitre II du titre II ;

— proxénétisme ou l'une des infractions prévues par les sections II et II bis du chapitre V du titre II ;

— conditions de travail et hébergement contraires à la dignité de la personne, prévus par la section III du chapitre V du titre II ;

2° Infractions prévues au livre III de la première partie du code pénal :

— vol, prévu par les sections 1 et 2 du chapitre Ier du titre Ier ;

— extorsion, prévue par la section 1 du chapitre II du titre Ier ;

— chantage, prévu par la section 2 du chapitre II du titre Ier ;

— escroquerie, prévue par la section 1 du chapitre III du titre Ier ;

— abus de confiance, prévu par la section 1 du chapitre IV du titre Ier ;

— détournement de gage ou d'objet saisi, prévu par la section 2 du chapitre IV du titre Ier ;

— organisation frauduleuse d'insolvabilité, prévue par la section 3 du chapitre IV du titre Ier ;

— recel et non-justification de ressources, prévus par les sections 1 et 2 du chapitre Ier du titre II ;

— atteintes aux systèmes de traitement automatisé de données, prévues au chapitre III du titre II ;

— blanchiment, prévu par la section 1 du chapitre IV du titre II.

3° Infractions prévues au livre IV de la première partie du code pénal :

— manquement au devoir de probité, prévu par la section III du chapitre II du titre III ;

— corruption active, trafic d'influence, soustraction ou détournement de biens publics, prévus par les sections 1 et 3 du chapitre III du titre III ;

— entraves à la saisine et à l'exercice de la justice, prévues par les sections 1 et 2 du chapitre IV du titre III ;

— atteintes à l'administration publique ou à l'action de la justice, prévues par les sections 1 et 2 du chapitre V du titre III ;

— violation d'interdiction de gérer ou d'interdiction professionnelle, prévue par l'article L. 434-40 ;

— faux, falsification de titres ou autres valeurs fiduciaires émises par l'autorité publique, falsification des marques de l'autorité et usage de tel faux, prévus par les chapitre Ier à IV du titre IV ;

— participation à une association de malfaiteurs, prévue par le titre V.

4° Infractions de travail illégal prévues par le chapitre unique du titre Ier au chapitre IV du titre II, le chapitre IV du titre III, le chapitre III du titre IV et le chapitre VI du titre V du livre II de la huitième partie du code du travail.

5° Infractions prévues aux livres II et VI du code de commerce :

— distribution de dividendes fictifs, présentation de comptes inexacts, abus de biens sociaux et abus de pouvoirs, prévus par le chapitre Ier, la section 2 du chapitre II, le chapitre III, le chapitre IV, le chapitre IV bis et le chapitre VI du titre IV du livre II ;

— banqueroute, détournement d'actifs et violation d'une interdiction de gérer, prévus par les sections 1 et 2 du chapitre IV du titre V du livre VI ;

6° Infraction de pratique de prêt usuraire, prévue par la section 1 du chapitre III du titre Ier du livre III du code de la consommation ;

7° Infractions à la législation et à la réglementation des relations financières avec l'étranger, prévues par le chapitre IV du titre XIV du code des douanes ;

8° Infraction de fraude fiscale, prévue par la section I du chapitre II du livre II de la troisième partie du code général des impôts ;

9° Infractions aux dispositions portant prohibition :

— des loteries, prévues par la loi du 21 mai 1836 portant prohibition des loteries ;

— de l'offre publique de paris hippiques, prévues par la loi du 2 juin 1891 ayant pour objet de réglementer l'autorisation et le fonctionnement des courses de chevaux ;

— de la tenue de maisons de jeux de hasard, prévues par la loi du 12 juillet 1983 relative aux jeux de hasard ;

— de l'offre publique de jeux ou de paris en ligne, prévues par la loi n° 2010 -476 du 12 mai 2010.

Par une juridiction étrangère, pour une infraction de même nature.

c) Des sanctions administratives prononcées à son encontre par la commission des sanctions de l'ARJEL en application de l'article 43 de la Loi.

Si l'entreprise est une personne morale

Elle justifie :

a) De l'existence et du lieu de son siège social ainsi que de sa forme juridique par la production de ses statuts ainsi que de tout autre élément de nature à établir le lieu du siège social, notamment par la production d'un extrait K bis ou d'un équivalent ;

b) De l'existence et du lieu du siège social de toutes sociétés qui la contrôle directement ou indirectement, de ses filiales ainsi que du lieu de situation de ses équipements ;

c) De l'identité de ses dirigeants par la production d'une copie de leur pièce d'identité ;

d) De l'adresse de ses dirigeants par la fourniture d'un justificatif de domicile ;

e) Des liens organiques des sociétés du groupe auquel elle appartient le cas échéant.

Elle informe l'ARJEL :

a) De sa dénomination sociale ;

b) Du ou des noms commerciaux qu'elle utilise ;

c) Dans l'hypothèse où elle est constituée en société par actions, de l'ensemble des personnes physiques ou morales détenant plus de 5 % de son capital ou de ses droits de vote ainsi que, le cas échéant, de la ou des personnes qui la contrôlent, directement ou indirectement, au sens de l'article L. 233-16 du code de commerce, notamment en produisant le schéma des participations précisant les pourcentages des détentions, directes et indirectes, ses statuts, tout pacte d'actionnaire, tout contrat aménageant les relations entre actionnaires ou tout contrat organisant son contrôle ; elle précise à l'ARJEL le lieu d'établissement de toute personne morale qui la contrôle au sens de l'article L. 233-16 du code de commerce ;

d) Des condamnations, devenues définitives, dont elle-même, son ou ses propriétaires ont, le cas échéant, fait l'objet depuis moins de dix ans, comme auteur ou complice :

Par une juridiction française, pour tout crime ou pour les délits dont la liste suit :

1° Infractions prévues au livre II de la première partie du code pénal :

— trafic de stupéfiants, prévu par la section 4 du chapitre II du titre II ;

— proxénétisme ou l'une des infractions prévues par les sections 2 et 2 bis du chapitre V du titre II ;

— conditions de travail et hébergement contraires à la dignité de la personne, prévus par la section 3 du chapitre V du titre II ;

2° Infractions prévues au livre III de la première partie du code pénal :

— vol, prévu par les sections 1 et 2 du chapitre Ier du titre Ier ;

— extorsion, prévue par la section 1 du chapitre II du titre Ier ;

— chantage, prévu par la section 2 du chapitre II du titre Ier ;

— escroquerie, prévue par la section 1 du chapitre III du titre Ier ;

— abus de confiance, prévu par la section 1 du chapitre IV du titre Ier ;

— détournement de gage ou d'objet saisi, prévu par la section 2 du chapitre IV du titre Ier ;

— organisation frauduleuse d'insolvabilité, prévue par la section 3 du chapitre IV du titre Ier ;

— recel et non-justification de ressources, prévus par les sections 1 et 2 du chapitre Ier du titre II ;

— atteintes aux systèmes de traitement automatisé de données, prévues au chapitre III du titre II ;

— blanchiment, prévu par la section 1 du chapitre IV du titre II ;

3° Infractions prévues au livre IV de la première partie du code pénal :

— manquement au devoir de probité, prévu par la section 3 du chapitre II du titre III ;

— corruption active, trafic d'influence, soustraction ou détournement de biens publics, prévus par les sections 1 et 3 du chapitre III du titre III ;

— entraves à la saisine et à l'exercice de la justice, prévues par les sections 1 et 2 du chapitre IV du titre III ;

— atteintes à l'administration publique ou à l'action de la justice, prévues par les sections 1 et 2 du chapitre V du titre III ;

— violation d'interdiction de gérer ou d'interdiction professionnelle, prévue par l'article L. 434-40 ;

— faux, falsification de titres ou autres valeurs fiduciaires émises par l'autorité publique, falsification des marques de l'autorité et usage de tel faux, prévus par les chapitres Ier à IV du titre IV ;

— participation à une association de malfaiteurs, prévue par le titre V ;

4° Infractions de travail illégal prévues par le chapitre unique du titre Ier au chapitre IV du titre II, le chapitre IV du titre III, le chapitre III du titre IV et le chapitre VI du titre V du livre II de la huitième partie du code du travail ;

5° Infractions prévues aux livres II et VI du code de commerce :

— distribution de dividendes fictifs, présentation de comptes inexacts, abus de biens sociaux et abus de pouvoirs, prévus par le chapitre Ier, la section 2 du chapitre II, le chapitre III, le chapitre IV, le chapitre IV bis et le chapitre VI du titre IV du livre II ;

— banqueroute, détournement d'actifs et violation d'une interdiction de gérer, prévus par les sections 1 et 2 du chapitre IV du titre V du livre VI ;

6° Infraction de pratique de prêt usuraire, prévue par la section 1 du chapitre III du titre Ier du livre III du code de la consommation ;

7° Infractions à la législation et à la réglementation des relations financières avec l'étranger, prévues par le chapitre IV du titre XIV du code des douanes ;

8° Infraction de fraude fiscale, prévue par la section I du chapitre II du livre II de la troisième partie du code général des impôts ;

9° Infractions aux dispositions portant prohibition :

— des loteries, prévues par la loi du 21 mai 1836 portant prohibition des loteries ;

— de l'offre publique de paris hippiques, prévues par la loi du 2 juin 1891 ayant pour objet de réglementer l'autorisation et le fonctionnement des courses de chevaux ;

— de la tenue de maisons de jeux de hasard, prévues par la loi du 12 juillet 1983 relative aux jeux de hasard ;

— de l'offre publique de jeux ou de paris en ligne, prévues par la loi n° 2010 -476 du 12 mai 2010.

Par une juridiction étrangère, pour une infraction de même nature.

e) Des sanctions administratives prononcées à son encontre ou à l'encontre de ses dirigeants par la commission des sanctions de l'ARJEL en application de l'article 43 de la Loi.

Moyens humains et matériels

L'entreprise justifie de ses moyens humains et matériels en fournissant tous documents relatifs :

a) Au nombre de ses salariés et à leurs fonctions (tableau de répartition du personnel par direction) ;

b) Aux prestataires et sous-traitants utilisés par le demandeur, en fournissant une liste ainsi que la nature des prestations réalisées ;

c) Aux locaux utilisés par le demandeur (usage, localisation, titre de l'occupation, superficie).

Informations complémentaires

Dans l'hypothèse où l'entreprise opère légalement dans son Etat d'établissement pour une même catégorie de jeux ou de paris en ligne, elle communique à l'ARJEL, à titre d'information, l'état du droit applicable et du régime de contrôle de l'activité de jeux ou de paris en ligne ainsi que les sanctions qui leur sont attachées.

Informations économiques,

financières et comptables

Eléments financiers et comptables

L'entreprise fournit à l'ARJEL les éléments suivants :

a) Les bilans, comptes de résultats, leurs annexes, la liasse fiscale et les rapports généraux et spéciaux des commissaires aux comptes des trois derniers exercices clos. Ces bilans, comptes de résultats et leurs annexes doivent être certifiés par l'expert comptable de l'entreprise ou, le cas échéant, par le commissaire aux comptes. Elle fournit également l'ensemble des rapports des commissaires aux comptes émis lors des trois derniers exercices.

Si, du fait d'une création récente, l'entreprise n'est pas en mesure de produire ces éléments pour les trois derniers exercices, elle fournit à l'ARJEL l'ensemble de ces documents pour les exercices clos, ainsi qu'une situation comptable intermédiaire, certifiée par l'expert comptable et/ou par le commissaire aux comptes le cas échéant. Cette situation comptable intermédiaire doit être comparable sur la forme comme sur le fond avec le dernier exercice clos.

Si l'entreprise a moins d'un an d'existence au moment du dépôt de son dossier d'agrément, elle produit un bilan d'ouverture certifié par un expert comptable et/ou un commissaire aux comptes le cas échéant ainsi qu'une situation comptable intermédiaire incluant des annexes et certifiée par l'expert comptable et/ou le commissaire aux comptes le cas échéant ;

b) Le demandeur transmet les comptes et annexes du dernier exercice clos de toute personne ou entité détenant le contrôle de l'entreprise, au sens de l'article L. 233-16 du code de commerce. L'entreprise fournit les comptes consolidés et les annexes correspondantes pour le dernier exercice clos de tout périmètre de consolidation dans lequel elle est intégrée ;

c) Un plan d'affaires synthétique des activités développées sur son site en.fr, tel que mentionné à l'article 24 de la Loi, relatif à l'exercice comptable de l'année de la demande d'agrément et au moins à l'exercice comptable suivant. Ce plan d'affaires doit être détaillé pour les catégories de jeux ou de paris pour lesquelles l'entreprise demande l'agrément et par support de paris. Il doit être accompagné des principales hypothèses retenues ;

d) Les tableaux de trésorerie des trois derniers exercices et un plan de trésorerie relatif au moins à l'année de la demande d'agrément et à l'exercice comptable suivant. Ils doivent être accompagnés des principales hypothèses retenues ;

e) Les engagements hors bilan, y compris les cautions bancaires, à la date de la demande d'agrément certifiés par l'expert comptable et/ou par le commissaire aux comptes le cas échéant ;

f) Une attestation fiscale et une attestation sociale délivrées par les organismes compétents au 31 décembre de l'année précédant la demande d'agrément.

g) Un relevé d'identité bancaire (RIB) ou IBAN justifiant l'ouverture d'un compte dans un établissement de crédit d'un Etat membre de la Communauté européenne, ou un Etat partie à l'Accord sur l'Espace économique européen ayant conclu avec la France une convention contenant une clause d'assistance administrative en vue de lutter contre la fraude et l'évasion fiscale, dédié exclusivement aux opérations d'encaissement et de paiement liées aux jeux ou paris offerts à partir de son site.fr.

Représentation fiscale

L'entreprise indique, lorsqu'elle n'est pas établie en France, le représentant fiscal établi en France qu'elle accrédite conformément à l'article 302 bis ZN du code général des impôts auprès de l'administration fiscale aux fins de remplir les formalités lui incombant et d'acquitter à sa place les prélèvements dus.

Elle fournit le RIB de ce représentant et en précise le nom et l'ensemble des coordonnées.

Elle précise l'organisation lui permettant d'assurer la déclaration et le paiement des versements de toute nature dus au titre de l'activité pour laquelle elle sollicite l'agrément.

Ces déclarations faites auprès de l'ARJEL ne valent pas accréditation du représentant fiscal. Cette accréditation doit être faite auprès des services des impôts des entreprises compétents.

Garanties financières

L'entreprise communique l'ensemble des informations comptables et financières de nature à attester sa solidité financière et sa capacité à assumer les investissements nécessaires au respect de ses obligations légales et réglementaires. Elle décrit et justifie notamment des moyens qu'elle entend mettre en œuvre pour faire face à ses engagements financiers lors de sa phase de développement (type de financement, calendrier, montant estimé, degrés d'avancement).

Informations relatives au site de jeux en ligne

5.1. **L'entreprise justifie de l'obtention au moins d'un nom de domaine de premier niveau comportant la terminaison « .fr » par la production d'un certificat d'enregistrement.** Elle déclare, le cas échéant, tous les autres noms de domaine de premier niveau comportant la terminaison « .fr » qu'elle entend exploiter pour l'accès à son site de jeux en ligne et fournit les pièces justifiant des enregistrements correspondants.

5.2. Elle présente la nature du site de jeux en ligne qu'elle entend exploiter, et notamment l'ensemble des activités et des prestations proposées.

5.3. Elle expose les caractéristiques (nombre de pages, plan du site, marques, HTML, site en marque blanche), les modalités d'accès et d'exploitation, d'organisation et de sous-traitance de son site (Objet du site : généraliste ou spécialisé ; caractéristiques : pages d'entrées, nombres de pages, types d'onglets ; modalités d'exploitation).

5.4. Elle précise si elle entend proposer des espaces publicitaires à des annonceurs sur son site.

5.5. Le cas échéant, elle fournit les copies non biffées des contrats de licence et des contrats d'affiliation qu'elle a conclus.

5.6. Le cas échéant, elle indique le nom de ses sous-traitants et fournit la copie non biffée des contrats de sous-traitance qu'elle a conclus pour l'exploitation de son site.

Informations relatives aux opérations de jeux

ou de paris en ligne proposées

6.1. L'entreprise précise les types de jeux ou de paris qu'elle propose au public, leur nature (paris à cotes fixes ou mutuels, paris en direct), leurs caractéristiques et leurs modalités d'exploitation, et fournit les règlements des jeux et paris qu'elle propose.

6.2. Elle fournit les copies non biffées des contrats de fourniture ou de sous-traitance d'opérations de jeu ou de paris en ligne qu'elle a conclus. Elle fournit également les copies non biffées des contrats la liant à d'autres entreprises exerçant une activé de jeux et paris en ligne.

6.3. Elle fournit à l'ARJEL la liste des sites affiliés.

6.4. Elle justifie de son aptitude à maintenir la conformité des jeux qu'elle propose au droit applicable, notamment en justifiant de la mise en place de veilles juridiques.

6.5. Elle indique le nom et les coordonnées en France de la personne responsable du maintien de la conformité des jeux proposés au droit applicable.

6.6. Elle fournit les contrats qu'elle propose aux joueurs ainsi que les conditions générales de vente et de services.

6.7. Elle décrit la procédure de réclamation gratuite qu'elle met en place au bénéfice des joueurs.

Informations relatives aux comptes joueurs

L'entreprise sollicitant l'agrément justifie des procédures qu'elle met en œuvre afin de répondre aux obligations prévues par les articles 17 et 18 alinéa 1 de la Loi.

Informations relatives à la lutte contre les activités frauduleuses ou criminelles, en particulier le blanchiment de capitaux et le financement du terrorisme

8.1. L'entreprise expose les moyens de contrôle qu'elle entend mettre en place pour prévenir et lutter contre les activités frauduleuses ou criminelles.

8.2. S'agissant de la lutte contre le blanchiment de capitaux et le financement du terrorisme, l'entreprise expose les moyens qu'elle entend mettre en œuvre pour satisfaire à :

— ses obligations de vigilance ;

— son obligation de déclaration à Tracfin des opérations dont elle sait, soupçonne ou a de bonnes raisons de soupçonner qu'elles participent du blanchiment de capitaux ou du financement du terrorisme ;

— ses procédures et son contrôle interne (système d'évaluation et de gestion des risques ; information et formation régulière de ses personnels), en référence aux dispositions du titre VI du livre V du code monétaire et financier.

Informations relatives à la lutte contre le jeu excessif ou pathologique

9.1. L'entreprise expose les moyens qu'elle entend mettre en place pour prévenir et lutter contre les comportements de jeu excessif ou pathologique.

9.2. Plus précisément, elle décrit l'ensemble des modérateurs de jeu qu'elle entend mettre en place sur son site conformément à l'alinéa 2 de l'article 26 de la loi.

9.3. En outre, l'entreprise expose les procédures qu'elle entend mettre en place et les moyens auxquels elle entend recourir pour répondre aux exigences de l'alinéa 1 de l'article 26 de la Loi.

Prévention des conflits d'intérêts

10.1. L'entreprise transmet à l'ARJEL les contrats de partenariat qu'elle a, le cas échéant, conclus avec des personnes physiques ou morales organisant des courses hippiques, compétitions ou manifestations sportives ou y prenant part.

10.2. L'entreprise déclare à l'ARJEL si son propriétaire, l'un de ses dirigeants, mandataires sociaux ou membres du personnel détient un intérêt, personnel ou lié à sa participation dans une personne morale, dans une course hippique, compétition ou manifestation sportive.

10.3. L'entreprise transmet à l'ARJEL la liste des organisateurs et parties prenantes à une compétition ou manifestation sportive sur lesquels elle détient le contrôle au sens de l'article L. 233-16 du code de commerce, directement ou indirectement au sens de l'article 32 de la Loi. A cet effet, elle transmet à l'ARJEL tout document relatif à ce contrôle et notamment le schéma des participations précisant les pourcentages de détention, directe et indirecte, dans des sociétés ainsi que tout pacte d'actionnaire, tout contrat aménageant les relations entre actionnaires (actionnariat, droit de vote...) ou tout contrat organisant le contrôle.

10.4. L'entreprise déclare à l'ARJEL si elle est contrôlée au sens de l'article L. 233-16 du code de commerce, directement ou indirectement au sens de l'article 32 de la Loi, par un organisateur ou une partie prenante à une compétition ou manifestation sportive.

10.5. Elle communique à l'ARJEL les clauses de son règlement intérieur ou de son contrat de travail type (dirigeants, mandataires sociaux, employés) stipulant l'interdiction d'engager à titre personnel, directement ou par personne interposée, des mises sur les jeux ou paris qu'elle propose.

10.6. Elle communique également à l'ARJEL les clauses de son règlement intérieur ou de son contrat de travail type (dirigeants, mandataires sociaux, employés) stipulant l'obligation pour le

cocontractant de déclarer un intérêt personnel ou lié à sa participation dans une personne morale, qu'il détient dans une course hippique, compétition ou manifestation sportive, sur laquelle l'entreprise organise des jeux ou des paris.

Informations relatives à l'architecture du système d'information

Définitions

11.1.1. On entend par frontal le support matériel d'archivage des données transitant entre le joueur et l'opérateur, et qui comprend un capteur et un coffre-fort.

11.1.2. On entend par système d'information :

— les différents modules du frontal ;

— l'ensemble des composants, aux niveaux système, réseau et applicatif et, plus généralement, tout système ou application susceptible d'interagir avec les plates-formes de jeux de l'opérateur.

Informations relatives au frontal

Au moment du dépôt de son dossier de demande d'agrément, l'entreprise expose à l'ARJEL, de façon détaillée, les mesures qu'elle prend pour que son frontal permette la captation et la sauvegarde de la totalité des données qu'il doit servir à recueillir.

Elle fournit l'identité et les coordonnées du prestataire ayant réalisé le coffre-fort et du prestataire ayant réalisé le capteur.

Avant de débuter son activité, l'opérateur agréé déclare à l'ARJEL que son frontal est en mode fonctionnement.

Les informations relatives au frontal comportent obligatoirement les éléments suivants :

Description générale du frontal :

— stratégie employée ;

— architecture générale ;

— localisation physique du frontal ;

— type d'hébergement réalisé ;

— production du ou des contrats d'hébergement ;

— politique de sécurité.

Description détaillée du frontal relative à la partie génération des traces :

— stratégie détaillée employée pour le capteur ;

— architecture technique et fonctionnelle détaillée ;

— le cas échéant, désignation des sous-traitants ayant développé les différents modules du frontal ;

— spécification des interfaces et relais « front-end » ;

— stratégie employée vis-à-vis de la très haute disponibilité demandée ;

— fourniture des codes sources ;

— politique de sécurité réalisée ;

— analyse de risques réalisés ;

— liste et résultats des tests d'audits effectués ;

— documents d'exploitation ;

— procédures mises en place notamment en ce qui concerne la protection contre les accès non autorisés.

Description détaillée du frontal relative au stockage sécurisé des traces :

— stratégie détaillée employée pour la création des traces ;

— architecture technique et fonctionnelle détaillée ;

— désignation des sous-traitants ou fournisseurs éventuels ;

— spécification détaillée ;

— précision des différents algorithmes employés ;

— spécification précise du déroulement de la cérémonie de clés nécessaire ;

— spécification et rôle des bi-clés utilisées ;

— politique de sécurité ;

— analyse de risques effectués ;

— rapports de tests effectués ;

— codes sources ;

— documents d'administration et d'exploitation ;

— procédures mises en place notamment en terme de protection contre les accès non autorisés ;

— procédures mises en place notamment en terme de protection contre les accès non autorisés.

Fourniture du certificat de sécurité a minima de premier niveau du coffre-fort (ou fourniture du calendrier d'obtention accompagné d'une note du centre d'évaluation ou du centre de certification attestant que la procédure de certification a été engagée).

Description détaillée des mécanismes d'authentification et de confidentialité mis en place (entre le joueur et le frontal, entre les différents modules du frontal, entre le frontal et la plate-forme).

Description détaillée de la cérémonie envisagée pour l'initialisation du coffre.

Description détaillée des mécanismes d'authentification des personnes physiques au coffre.

Description détaillée de l'outil de collecte à distance des fichiers de traces.

Description détaillée de l'outil de validation et d'extraction des fichiers de traces.

Description détaillée des mesures de sécurisation du frontal.

Description détaillée des fonctions d'administration des utilisateurs du frontal :

— spécifications détaillées ;

— code source ;

— rapports de tests.

Description détaillée des fonctions de redirection des connexions de joueurs.

Description détaillée du site.fr mis en place :

— hébergeur ;

— localisation ;

— code source ;

— politique de sécurité ;

— analyse de risques ;

— procédures mises en place.

Procédures d'homologation et de vérification

Procédure d'homologation des logiciels de jeux et de paris

L'entreprise communique le code source de chaque logiciel de jeux et de paris destiné à être utilisé par les joueurs et les parieurs français ainsi que le code source de l'éventuel générateur de nombre aléatoire.

Elle communique les trois rapports spécifiques d'analyse des codes sources suivants, réalisés par des prestataires de son choix dont elle fournit les coordonnées :

— un rapport d'analyse détaillée des vulnérabilités de sécurité du code source. Il a pour objet de décrire la méthode utilisée pour l'analyse du code, de constater l'ensemble des vulnérabilités identifiées, d'exposer chaque vulnérabilité techniquement et d'expliquer l'impact précis de l'exploitation de chaque vulnérabilité identifiée ;

— un rapport d'analyse spécifique du générateur de nombre aléatoire Il a pour objet d'exposer les éventuelles vulnérabilités du code et de préciser le niveau de qualité intrinsèque de ce générateur aléatoire. Il a par ailleurs pour objet de vérifier les caractéristiques suivantes liées au caractère aléatoire du générateur (selon la méthode de Bruce Schneier) :

— les mécanismes de génération doivent avoir subi avec succès différents tests statistiques démontrant leur caractère aléatoire ;

— les données aléatoires générées doivent être non prévisibles : il doit être impossible de prédire la donnée générée suivante même si l'on a connaissance de l'algorithme ou du matériel de génération et de toutes les données précédemment générées ;

— les séries de données générées ne doivent pas être reproductibles : si le générateur aléatoire est activé avec les mêmes paramètres en entrée, il doit générer une nouvelle séquence de données ;

— un rapport d'analyse certifiant que les règles implémentées dans le logiciel de jeu sont bien conformes au jeu tel qu'il est présenté au joueur. Les règles sont jointes au rapport.

L'ARJEL rend une décision sur l'homologation des logiciels de jeux distincte de celle relative à la demande d'agrément.

Un opérateur agréé ne peut pas débuter son activité de jeu sans homologation des logiciels de jeu et de paris.

Vérification initiale de la plate-forme de jeu

L'entreprise communique un rapport d'analyse des vulnérabilités techniques. Il a pour objet de constater l'ensemble des vulnérabilités identifiées sur la plate-forme de jeu, d'exposer leur impact et de proposer un plan d'action. Elle précise en outre les coordonnées du prestataire auteur de ce rapport.

Informations générales

Les différents éléments demandés ci-après concernent l'ensemble des systèmes d'information de l'entreprise tels que définis au paragraphe 11.1.2 ci-dessus. Si certaines briques de ces systèmes

n'étaient pas opérationnelles lors du dépôt de la demande d'agrément, l'entreprise devra en indiquer les raisons et préciser le calendrier de mise en œuvre de ces systèmes ainsi que celui de remise des différents éléments demandés ci-dessous.

Politique et organisation des systèmes d'information

L'entreprise décrit :

— les différentes directions qui la composent, avec leurs missions précises ;

— les éventuels services déconcentrés qui lui sont rattachés, avec leurs fonctions respectives et leurs implantations géographiques.

L'entreprise décrit :

— le schéma de son organisation de conduite des projets et de mise en œuvre des systèmes d'information ;

— sa politique générale informatique ;

— son schéma directeur informatique.

Description des systèmes d'information

L'entreprise précise :

— les centres d'exploitation et de supervision informatiques et réseau (localisation, application, personnel) ;

— les centres d'hébergement (localisation, type d'hébergement) ;

— les centres d'interconnexion (types) ;

— les centres opérationnels.

Pour les plates-formes de jeux, le frontal et l'ensemble des systèmes d'information afférents à ceux-ci, l'entreprise précise :

— la ou les fonctions assurées ;

— le type de données traitées ;

— l'entreprise ou l'autorité responsable de son exploitation ;

— le fournisseur d'accès ;

— l'hébergeur.

Elle fournit la liste des principales applications installées sur les plates-formes de jeux.

Pour chacune de ces applications, l'entreprise précise :

— la ou les fonctions assurées ;

— le type de données traitées ;

— l'entreprise ou l'autorité d'exploitation désignée ;

— ses implantations, son architecture et les réseaux utilisés (internet ou réseau dédié) ;

— le cas échéant, les moyens de chiffrement mis en œuvre ;

— l'importance de sa fonction (de « outil facilitant le travail » à « outil indispensable ») ;

— l'importance de sa disponibilité (de « aucun effet » à « effet bloquant » en cas d'arrêt total ou partiel du système) ;

— l'importance de l'intégrité des données (de « aucun effet » à « effet bloquant » en cas de modification de données) ;

— l'importance de la confidentialité des données (de « aucun effet » à « effet bloquant » en cas de divulgation de données) ;

— la durée de vie prévue.

Si des projets sont en cours, l'opérateur fournit les mêmes renseignements que pour ceux en service et précise les maîtrises d'ouvrage et les maîtrises d'œuvre.

Ressources humaines dédiées à la sécurité informatique

L'entreprise décrit l'organisation mise en place pour assurer la sécurité des systèmes d'information, ainsi que la sécurité physique des locaux ;

Elle précise, le cas échéant, l'existence des fonctions suivantes et fournit les informations demandées :

— responsable sécurité du service d'information : définition précise des responsabilités, degré de formalisation, nombre d'adjoints et rattachement hiérarchique ;

— autorité d'exploitation du système d'information (SI) (ou fonction équivalente) : définition précise des responsabilités, degré de formalisation et, le cas échéant, nature des responsabilités en matière de sécurité des systèmes d'information (SSI) ;

— juriste spécialisé en SSI : nombre et rattachement hiérarchique ;

— auditeurs internes en SSI : nombre et rattachement hiérarchique ;

— fonction de contrôle interne en SSI : nombre et rattachement hiérarchique ;

— fonction support en SSI : nombre et rattachement hiérarchique ;

— fonction opérationnelle en SSI : nombre et rattachement hiérarchique) ;

— fonction de conception en SSI : nombre et rattachement hiérarchique.

Elle communique, le cas échéant, ses tableaux de bord SSI.

Elle communique, le cas échéant, son budget SSI. A défaut, elle en donne une estimation et précise la proportion qu'il représente par rapport au budget des SI.

Pilotage des systèmes d'information

L'entreprise précise les phases du cycle de vie des systèmes au cours desquelles la sécurité des systèmes d'information est prise en compte.

A cet effet, elle fait notamment état de la manière dont les aspects liés à la sécurité sont pris en compte dans les expressions des besoins relatifs au développement (en interne ou sous-traité) et au maintien en condition des systèmes d'information et des applications (application des correctifs notamment).

Elle précise également si les applications développées ont une durée de vie estimée.

L'entreprise communique des extraits du cahier des clauses techniques particulières (CCTP) ainsi que les clauses relatives à la sécurité.

Elle fait état, le cas échéant, de la procédure de recette SSI relative aux projets de systèmes d'information avant leur mise en service et précise la proportion des systèmes d'information ayant effectivement fait l'objet d'une telle recette.

Elle précise, le cas échéant, les modalités de mise en œuvre de tout examen formalisé d'impact sur la sécurité d'un SI ou sur la mise en exploitation d'un nouveau composant (modèle de serveur, système d'exploitation, application, données, etc.).

Elle précise les applications dont elle est titulaire des droits d'auteur.

Elle communique, le cas échéant, les études de risques qu'elle a réalisées. Elle en précise la méthodologie.

Elle précise, le cas échéant, les modalités d'identification et de classification des composants sensibles (y compris les données) et la méthodologie y afférente.

Elle fait état, le cas échéant, des périmètres, conditions, modalités et résultats de toutes évaluations ou certifications.

Elle précise les métiers faisant appel à la sous-traitance ou à l'externalisation (notamment,

hébergement Web, infogérance, sécurité...).

Elle précise, le cas échéant, la nature, la périodicité, les acteurs et la méthodologie des audits SSI réalisés sur les systèmes d'information et les applications. Elle en communique les comptes rendus et les principales recommandations. Elle précise les modalités de décision des mesures correctrices, et celles de leur mise en œuvre et du contrôle de leur bonne exécution. Elle indique la proportion des mesures réellement appliquées.

Elle précise la proportion de son personnel ayant été sensibilisé ou formé à la SSI dans les chaînes SI et SSI et parmi les utilisateurs. Elle précise également s'il existe une gestion et un suivi régulier de la compétence de chacun.

Elle expose comment elle prend en compte les aspects réglementaires, notamment s'agissant des données personnelles (CNIL).

Elle expose, le cas échéant, le mode de fonctionnement de son centre opérationnel chargé de la SSI. Elle en précise notamment le rattachement hiérarchique, le régime de veille et l'effectif de permanence. A défaut, elle précise les modalités de veille et de déclenchement des alertes.

Elle expose, le cas échéant, toute procédure d'astreinte SSI. Elle en précise notamment l'organisation, le niveau de personnel et les modalités de contact.

Elle communique, le cas échéant, tout document faisant état des procédures mises en place en vue de traiter les cas d'incident et de détection de fraude. **Elle précise le niveau de diffusion de ces documents ainsi que les modalités d'alerte prévues.**

Elle fait état, le cas échéant, des incidents de SSI ou des fraudes qu'elle aurait pu constater. Elle en précise les occurrences (notamment l'identification des sources d'entrée et du niveau) et la gestion qui en a été faite.

Informations détaillées

Les différents éléments demandés ci-après concernent l'ensemble des systèmes d'information de l'entreprise tels que définis au paragraphe 11.1.2 ci-dessus. Si certaines briques de ces systèmes n'étaient pas opérationnelles lors du dépôt de la demande d'agrément, l'entreprise devra en indiquer les raisons et préciser le calendrier de mise en œuvre de ces systèmes ainsi que celui de remise des différents éléments demandés ci-dessous.

Informations de niveau organisationnel

Politique et schéma directeur de la sécurité

des systèmes d'information

L'entreprise fournit un schéma directeur en SSI (ou un document équivalent). Elle en précise la date de début d'application, et la périodicité des mises à jour. Elle précise également si le schéma directeur SSI est intégré dans le schéma directeur informatique. Elle en fournit les deux dernières versions.

Elle précise ses orientations stratégiques ainsi que le niveau de réalisation des actions en découlant.

Elle expose sa politique de sécurité en matière de systèmes d'information et précise à cet effet son périmètre d'application et les éléments ci-après mentionnés. Elle communique, le cas échéant, tout document en faisant état. Cette politique de sécurité devra comprendre les éléments suivants :

— éléments stratégiques :

— le périmètre d'application de la politique de sécurité, par exemple en termes de domaines d'activités ou de systèmes d'information ;

— les enjeux et orientations stratégiques, à travers la formalisation des enjeux liés au périmètre précédemment défini ;

— les aspects légaux et réglementaires liés au périmètre d'application de la politique de sécurité ;

— une échelle de besoins qui comportera une pondération et des valeurs de référence selon les critères de sécurité choisis, ainsi qu'une liste d'impacts enrichis d'exemples ;

— une description des besoins de sécurité des domaines d'activité de l'opérateur, selon l'échelle de besoins présentée dans la partie précédente ;

— une analyse des menaces retenues et non retenues pour le périmètre de l'étude, avec des justifications.

— règles de sécurité, par thème :

— organisation : organisation de la SSI, gestion des risques, sécurité et cycle de vie, assurance et certification, évolution de la PSSI ;

— mise en œuvre : aspects humains, plan de secours, gestion des incidents, sensibilisation et formation, exploitation, sécurité physique ;

— technique : identification/authentification, contrôle d'accès logique, journalisation, chiffrement.

Elle expose les déclinaisons techniques détaillées des éléments exigés par sa politique de sécurité. Elle précise le lien entre la politique de sécurité et toutes les procédures liées aux systèmes d'information ainsi que les moyens (organisationnels et techniques) de sécurisation et leur suivi dans le temps.

Elle expose les exigences de sécurité qu'elle impose aux divers sous-traitants avec lesquels des relations contractuelles sont établies. Elle communique les clauses contractuelles types.

Elle précise, le cas échéant, les contrôles qu'elle exerce auprès de ses sous-traitants afin d'assurer un maintien du niveau de sécurité de ses plates-formes et systèmes d'information.

Procédures d'administration et d'exploitation

L'entreprise communique toute documentation faisant état de la procédure de gestion de ses systèmes d'information. Cette documentation précise les éléments suivants :

— une description fonctionnelle du SI (elle peut être intégrée dans la politique de sécurité) précisant les composants de l'interconnexion et les flux devant transiter au travers de celle-ci ;

— une description technique du SI issue de l'étude d'architecture (incluant notamment les composants techniques, adressage/nommage, flux techniques [protocoles] nécessaires avec leur sens) et comprenant des éléments factuels (licences des logiciels utilisés, contrats de maintenance, configurations à jour des équipements, état des modifications effectuées) ;

— une liste de procédures d'exploitation des composants de l'interconnexion (qui peuvent être incluses ou non dans une déclinaison technique de politique de sécurité) ;

— des procédures d'exploitation classiques comme la gestion des comptes et mots de passe, la gestion de la configuration des composants, la gestion de sauvegardes ;

— des procédures spécifiques liées à la sécurité.

Les procédures d'exploitation suivantes seront notamment transmises par l'entreprise :

— procédures de gestion des journaux ;

— procédures de gestion des alertes ;

— procédures de mise à jour régulière de tous les composants (systèmes d'exploitation, applications, routeurs, etc.) ;

— procédures de gestion des composants à mise à jour fréquente (antivirus, systèmes de détection d'intrusion, le cas échéant) ;

— procédures de mise à jour en cas d'édition d'un correctif de sécurité critique ;

— procédures pour la mise en sécurité des systèmes en cas d'urgence ou de danger imminent ;

— procédures d'exploitation des composants du SI (serveurs, routeurs) ;

— procédures d'exploitation des comptes et mots de passe ;

— procédures de gestion des composants infogérés ;

— procédures relatives à la sécurité physique (gardiennage, etc.) ;

— procédures de gestion des sauvegardes et des restaurations ;

— procédures de veille technologique ;

— procédures pour la téléadministration ;

— procédures de gestion des tableaux de bord SSI.

Informations techniques

Description des systèmes d'information

L'entreprise décrit les éléments suivants pour chacun des systèmes mentionnés dans la section 11.4.2 « Description des systèmes d'information » :

Elle décrit l'architecture du réseau en précisant notamment comment elle a été définie. Elle fait également état de son historique.

Elle fournit les éléments suivants :

— un schéma technique du réseau ;

— la liste des différents flux associés ;

— la liste des zones de sensibilités différentes ;

— la liste des interconnexions de ces zones, avec une explication ;

— la liste des liens vers l'extérieur (lignes dédiées, interconnexions de réseaux...) et les accès distants possibles depuis l'extérieur (modems analogiques, RNIS, Internet, etc.) ;

— l'entreprise précise les contrats conclus avec les fournisseurs d'accès ;

— l'entreprise précise comment les diverses fonctions et les services sont implantés ;

— l'entreprise précise les technologies mises en œuvre.

Elle communique le « dossier de définitions ». Celui-ci s'entend du dossier regroupant (i) les informations techniques, incluant notamment les spécifications concernant l'architecture du système, les documentations des matériels ou des logiciels, les configurations (règles de filtrage, DNS, pare-feu, messagerie, etc.), (ii) le plan d'adressage, et (iii) la liste descriptive précise de tous les éléments (matériels et logiciels, versions, contrat de maintenance).

Architecture réseau

L'entreprise décrit la segmentation de ses systèmes d'information. Elle décrit également le filtrage réseau de ses systèmes d'information en accord avec le principe de défense en profondeur, notamment au niveau des réseaux de services, d'administration et de supervision des plates-formes. Cette description est conforme aux descriptions fonctionnelles et techniques décrites dans la section 11.4.2 « Description des systèmes d'information ».

Elle décrit le cloisonnement du réseau qu'elle applique entre les zones suivantes :

—les zones dédiées aux serveurs, avec un cloisonnement supplémentaire en fonction du niveau

de sensibilité identifié pour chacun par la politique de sécurité :

— les serveurs métie (serveurs d'applications, systèmes de gestion de base de données) ;

— les serveurs d'infrastructu (serveurs d'authentification, serveurs de messagerie, serveurs de fichiers, serveurs de distribution de logiciels) ;

— les équipements d'infrastructure réseau (routeurs, commutateurs) ;

— les serveurs de tests, de développement et de préproduction ;

— la zone des équipements dédiés à l'administration, l'exploitation et la supervision du système d'information. Cette zone qui héberge notamment les postes de travail des administrateurs et les serveurs de supervision devra faire l'objet d'une attention particulière compte tenu des accès privilégiés qu'ils sont susceptibles d'accorder sur les ressources les plus critiques du SI ;

— la ou les zones dédiées aux postes de travail des utilisateurs, avec un découpage supplémentaire dont la granularité pourra varier selon les missions des différents services métiers et la criticité de l'information dont ils ont la responsabilité.

Elle expose sa politique de filtrage réseau et décrit les règles de filtrage en termes de liste blanche.

Elle décrit les mécanismes de cloisonnement réseau déployés (filtrage IP, filtrage applicatif, VLAN, 802.1X, NAP/NAC, etc.).

Gestion de la disponibilité

L'entreprise communique ses contrats de maintenance.

Elle expose sa politique à l'égard des fournisseurs de matériels et de logiciels (notamment contractualisation, délai maximum d'intervention en cas d'incident, délai maximal d'approvisionnement en cas de défaillance matérielle de l'un des équipements, ou en cas d'ajout de matériel sur la plate-forme. Elle communique les contrats de maintenance.

Elle expose les mécanismes de sécurité qu'elle entend mettre en œuvre afin d'assurer une défense contre les attaques classiques sur IP et les protocoles associés, en particulier par rapport aux attaques en déni de service réseau.

Elle décrit les mesures techniques prises en termes de résilience réseau de ses systèmes d'information, notamment au regard de la lutte contre les attaques en déni de service (distribuées ou non, par épuisement de bande passante, ou encore de ressources système) au niveau des plates-formes de jeux et du frontal. Elle décrit notamment les procédés techniques mis en œuvre (équilibrage de charge, ajustement des TTL DNS, réadressage IP dynamique des plates-formes et du frontal) et les mesures organisationnelles associées (remontée d'alerte en cas d'attaque, **protocole d'accord avec les FAI pour la lutte contre les DDOS**, etc.).

Elle décrit les solutions qu'elle met en œuvre pour éviter ou détecter, le cas échéant, les attaques et intrusions sur ses systèmes d'information.

Gestion des mises à jour

L'entreprise expose sa politique d'application des correctifs de sécurité. Elle expose sa politique en cas de vulnérabilité identifiée et d'absence de correctifs.

Elle décrit le processus d'application des correctifs, et notamment en cas de régression constatée. Elle expose notamment les procédures techniques permettant un retour en arrière dans le cas où le correctif provoquerait une éventuelle régression.

Gestion des échanges

Confidentialité et authenticité des flux d'administration :

L'entreprise décrit les procédés cryptographiques permettant de garantir l'authentification des composants, la confidentialité et l'authenticité des communications suivantes :

— les communications entre opérateur et l'ARJEL ;

— les communications réseaux entre joueurs et opérateur ;

— les communications réseaux entre les modules au sein du frontal.

Elle décrit les mécanismes reposant sur des algorithmes de chiffrement reconnus et des protocoles normalisés par l'IETF (IPsec, TLS, SSH, etc.).

Elle décrit l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux au sein de ses plates-formes de jeux et du frontal : ces flux concernent les administrateurs faisant partie du personnel de l'opérateur tels les exploitants, par exemple, les administrateurs externes tels ceux qui assurent la télémaintenance des matériels, etc.

Authentification des administrateurs :

L'entreprise décrit les mécanismes d'accès aux fonctions d'administration de la plate-forme de jeu et du frontal.

Pour ses personnels exploitants, elle précise les mesures mises en œuvre lui permettant de garantir un haut niveau de sécurité dans la gestion des secrets d'authentification (notamment robustesse des mots de passe, changement périodique, authentification forte).

Elle précise si ses personnels exploitants utilisent régulièrement ou occasionnellement (astreintes, par exemple) des accès distants pour administrer tout ou partie des systèmes. Le cas échéant, l'entreprise décrit précisément les mécanismes mis en œuvre pour garantir la sécurité de ces accès distants, et le périmètre d'actions des intervenants accédant depuis l'extérieur.

Gestion des configurations

L’entreprise décrit les méthodes mises en place pour le suivi des évolutions logicielles des éditeurs de façon à être en mesure de se procurer les correctifs de sécurité mis à disposition régulièrement.

Elle décrit les moyens prévus permettant d’identifier et de prendre en compte les évolutions logicielles des constructeurs.

Elle décrit les mesures de sécurisation adoptées sur chacun des composants de sa plate-forme.

Elle décrit les moyens prévus pour gérer les différentes versions des fichiers de configuration ainsi que leur sauvegarde.

Elle décrit sa politique de vérification de l’intégrité de ses fichiers de configuration.

Gestion de la sécurité dans les cycles de développement

L’entreprise décrit sa gestion de la sécurité à chaque étape du cycle de développement de ses systèmes, dans les phases de définition, de développement, d’exploitation et d’utilisation, puis de maintenance et d’évolution.

Elle présente les mesures de contrôle et méthodes d’évaluation de ses développements à chaque étape d’un projet de développement. Elle communique, le cas échéant, le guide d’intégration de la sécurité des systèmes d’information dans les projets.

Elle présente son référentiel de développement sécurisé pour les projets dont elle assure le développement.

Elle communique, le cas échéant, les contrats conclus avec ses prestataires relatifs à la mise en place d’un référentiel de développement sécurisé pour les projets dont l’entreprise externalise la prise en charge.

Gestion des sauvegardes de données

L’entreprise décrit son service d’archivage en vue d’assurer la conservation de l’ensemble de ses données de traitement, et en particulier celles stockées dans le coffre-fort du frontal. Elle précise le type de support et le format de la sauvegarde.

Elle présente les mécanismes d’archivage ainsi que les moyens sécurisés de protection des archives qu’elle est capable de mettre en œuvre.

Elle décrit les modalités de son plan de sauvegarde. Elle précise en particulier les modalités et les délais de restauration d’une sauvegarde à la suite d’un incident ainsi que le ou les lieux de stockage des sauvegardes et les mesures de sécurité appliquées à ces lieux.

Gestion de données sensibles

L’entreprise décrit les procédures et mécanismes mis en place afin de protéger les données qu’elle traite, et notamment :

— les données nominatives et personnelles de ses clients ;

— les données et statistiques de jeu ou de certains joueurs dont la connaissance pourrait avantager un joueur ;

— les données de jeu « secrètes » (par exemple les cartes des autres joueurs, ou celles qui n'ont pas été retournées lors d'une partie de poker).

Gestion du générateur de nombres aléatoires

L'entreprise décrit les procédures et mécanismes mis en place afin de protéger le générateur de nombres aléatoires, et notamment :

— la surveillance de la série de nombres ;

— la protection d'une éventuelle graine de l'algorithme de génération de nombres aléatoires ;

— la protection de l'intégrité du logiciel.

Gestion de la journalisation technique et fonctionnelle

L'entreprise présente sa journalisation technique et fonctionnelle.

Elle décrit les traces sécurité qu'elle peut activer et les modalités d'analyse des traces qu'elle met en œuvre (périodicité, outils d'analyse utilisés...).

Elle précise le mode opératoire et la liste des journaux auxquels l'ARJEL aura accès (journaux de connexion locale ou des accès distants, journaux systèmes, journaux Web, journaux fonctionnels des applications, ou encore journaux générés par les SGBD, etc.).

Elle présente les moyens prévus pour la détection, le traitement et la notification des incidents ainsi que leurs modalités de gestion (y compris les procédures d'escalade).

Gestion des accès physiques

L'entreprise expose sa politique de gestion des accès physiques.

Elle expose la politique en matière de contrôle et décrit notamment les procédures mises en œuvre s'agissant de la vérification des candidats postulant à un poste sensible, de la gestion des confits d'intérêts, et des **modalités de mise en sécurité de l'information lors du départ de salariés de la société (récupération des badges, gestion des mots de passe, etc.).**

Elle présente l'ensemble des mesures de sécurité concernant son personnel.

Elle présente les moyens mis en œuvre aux fins de protection des locaux techniques.

Gestion de l'environnement physique

L'entreprise présente ses normes de protection incendie.

Elle décrit sa politique de redondance en alimentation électrique.

Elle décrit sa politique de surveillance H24 de ses sites d'exploitation.

Elle précise les plans de continuité d'activité et les plans de reprise d'activité qu'elle aura pu élaborer dans le cadre de son activité et les modalités qu'elle prévoit pour les adapter au contexte du frontal.

Equipe sécurité

L'entreprise décrit l'équipe sécurité chargée de surveiller tous les équipements réseau, systèmes et les applications.

Elle décrit les procédures mises en œuvre concernant l'équipe sécurité. Elle communique, le cas échéant, la charte de sécurité qui encadre cette activité.

Fait à Paris, le 17 mai 2010.

Le ministre du budget, des comptes publics
et de la réforme de l'Etat,
François Baroin
Le ministre de l'intérieur,
de l'outre-mer et des collectivités territoriales,
Brice Hortefeux
La ministre de la santé et des sports,
Roselyne Bachelot-Narquin
Le ministre de l'alimentation,
de l'agriculture et de la pêche,
Bruno Le Maire
La secrétaire d'Etat
chargée des sports,
Rama Yade