ENGAGEMENTS DORA

Les présents engagements DORA (ci-après les « Engagements DORA ») ont pour objet de compléter les Conditions Générales d'adhésion et d'utilisation du Portail ASPOne.fr (CGAU) **lorsque le Client, en tant qu'entité financière au sens du Règlement DORA, indique expressément à l'Editeur que tout ou partie des Services Hébergés désignés dans la Demande d'adhésion constituent des services TIC soumis au Règlement DORA. A défaut d'indication expresse en ce sens, les présents Engagements DORA ne sont pas applicables**. S'ils s'appliquent, en cas de contradiction ou de divergence éventuelle entre les CGAU et les Engagements DORA, ces derniers priment en ce qui concernent les Services TIC tels que définis ci-dessous.

1. DEFINITIONS

Les termes commençant par une majuscule et qui ne sont pas définis dans les présents Engagements DORA ont la signification qui leur est donnée dans les CGAU. Les présentes s'appliquent uniquement aux Services TIC tels que définis ci-après :

Autorités Compétentes : a le sens qui lui est donné dans le Règlement DORA (article 46).

Fonction(s) Critique(s) ou Importante(s) : désigne une fonction dont (i) la perturbation est susceptible de nuire sérieusement à la performance financière du Client, ou à la solidité ou à la continuité de ses services et activités, ou (ii) un Incident de l'exécution de cette fonction est susceptible de nuire sérieusement à la capacité du Client de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables du droit relatif aux services financiers. **Sauf indication expresse en ce sens fournie par le Client, les Services TIC fournis par l'Editeur ne soutiennent pas de Fonctions Critiques ou Importantes.**

Incident de sécurité : désigne un événement ou une série d'événements liés entre eux lié aux Services TIC que le Client n'a pas prévu qui compromet la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des Données ou sur les services fournis par le Client.

Incident de sécurité majeur : désigne un Incident de sécurité qui a une incidence négative élevée sur les réseaux et les systèmes d'information qui soutiennent les Fonctions Critiques ou Importantes du Client.

Services TIC : désigne ceux des Services fournis qui sont expressément soumis au Règlement DORA selon la qualification du Client au sein des Conditions Particulières.

TLPT (« threat-led penetration testing ») : désigne les tests de pénétration fondés sur les menaces, tels que décrits aux articles 26 et 27 du Règlement DORA.

2. LIEU DE REALISATION DES SERVICES ET SOUS-TRAITANCE

Conformément au Règlement DORA, les lieux, notamment les régions ou les pays, où les Services TIC sont fournis et où les Données seront traitées, y compris le lieu de stockage figurent dans le « Registre Portail ASPone.fr- RGPD ». Tout recours à d'autres sous-traitants ultérieurs ou de modification des lieux de stockage des Données doit faire l'objet d'une information écrite et préalable au Client.

Dans le cadre du respect du Règlement DORA (ainsi que les normes techniques s'y rapportant), l'Editeur s'engage, en ce qui concerne les contrats avec ses sous-traitants qui fournissent des Services TIC soutenant des Fonctions Critiques ou Importantes (ci-après au sens des seules présents Engagements DORA, les « Sous-traitants »), à :

- rester responsable envers le Client de la fourniture des Services TIC sous-traités ;
- surveiller les Services TIC qui soutiennent des Fonctions Critiques ou Importantes ou des parties significatives de celles-ci et qui ont été sous-traités, pour garantir le respect de ses obligations contractuelles ;
- évaluer les risques liés à la localisation des Sous-traitants et du lieu où les Services TIC soutenant des Fonctions Critiques ou Importantes sont fournis ;
- ce que la continuité des Services TIC soutenant des Fonctions Critiques ou Importantes soit assurée, même en cas de défaillance d'un Sous-traitant, conformément aux plans de continuité définis contractuellement par les présentes ;
- répercuter les normes de sécurité prévues par les présentes à ses Sous-traitants ;
- ce que les Sous-traitants accordent au Client et aux Autorités Compétentes les mêmes droits d'accès, d'inspection et d'audit que ceux accordés dans les présentes par l'Editeur et dans les mêmes conditions préalables ;
- ce que le Client dispose de droits de résiliation du Contrat dans les cas prévus à l'article "Résiliation" ci-après ;
- faire figurer des obligations similaires aux obligations visées à l'article "Coopération et audit" ci-après dans le contrat le liant au sous-traitant, afin que ce dernier coopère et permette l'accès à toute autorité de contrôle, aux informations relatives aux actions du sous-traitant, dans le cadre des Services TIC.

En cas de changement significatif dans les accords de sous-traitance relatifs aux services TIC soutenant des Fonctions Critiques ou Importantes, l'Editeur doit :

- Informer le Client en temps utile pour permettre au Client d'évaluer l'impact de ces changements sur les risques existants ou potentiels ainsi que la capacité de l'Editeur de Services TIC à respecter ses obligations contractuelles ;
- Le Client doit approuver les changements ou s'y opposer dans un délai de 15 jours.
- L'Editeur de Services TIC met en œuvre les changements significatifs qu'après avoir reçu une approbation explicite ou une absence d'injonction de la part du Client à la fin du délai susmentionné.

En cas de tels changements significatifs dans les arrangements de sous-traitances relatifs aux Services TIC soutenant des Fonctions Critiques ou Importantes, le Client doit évaluer les risques de ces derniers sous sa responsabilité. Si cette évaluation dépasse son niveau de tolérance au risque, celui-ci doit avant la fin du délai de préavis de 15 jours susmentionné :

- Informer par écrit l'Editeur des résultats de son évaluation ;
- S'opposer par écrit aux changements et demander leurs modifications avant leur mise en œuvre.

3. ASSISTANCE EN CAS D'INCIDENT LIE AUX SERVICES

L'Editeur fournit une assistance en cas d'Incident de sécurité lié aux Services TIC fournis au titre du Contrat. L'assistance fournie par le l'Editeur est facturée au Client conformément aux conditions suivantes : (i) si l'incident n'est pas exclusivement imputable à l'Editeur, au-delà de deux (2) jours ouvrés l'assistance sera facturée au Client, selon le tarif journalier suivant : 700€ HT/ jour ouvrés ; si l'Incident de sécurité est exclusivement imputable à l'Editeur, l'assistance est fournie au Client sans frais supplémentaire.

4. COOPERATION ET AUDIT

L'Editeur s'engage à coopérer pleinement le cas échéant avec les Autorités Compétentes et les autorités de résolution du Client, ainsi qu'avec toutes personnes mandatées par elles. Le

Client se réserve la possibilité de procéder à l'audit selon les modalités détaillées à l'article 18 « Audit » des CGAU.

5. DROITS DE RESILIATION ADDITIONNELS

Le Contrat pourra en outre être résilié par le Client conformément à l'article « Résiliation » des Conditions Générales dans l'un de cas suivants :

- L'Editeur a gravement enfreint les dispositions législatives ou réglementaires qui lui sont applicables au titre du Contrat ;
- Le suivi des risques liés à l'Editeur a révélé l'existence de circonstances susceptibles d'altérer l'exécution des Services TIC (en ce compris des changements significatifs affectant l'exécution du Contrat ou la situation juridique de l'Editeur) ;
- L'Editeur présente des faiblesses avérées liées à sa gestion globale du risque lié aux Services TIC, en particulier dans la manière dont il assure la disponibilité, l'authenticité, l'intégrité et la confidentialité des Données, qu'il s'agisse de données à caractère personnel ou autrement sensibles, ou de données à caractère non personnel ;
- L'Autorité Compétente ne peut plus surveiller efficacement le Client en raison des conditions du Contrat ou des circonstances qui y directement sont liées.

Dans le cadre du respect du Règlement DORA, lorsque l'Editeur a recours à des Sous-traitants, le Client a le droit de résilier le Contrat avec l'Editeur dans les cas supplémentaires suivants liés aux Services TIC, pour manquement de l'Editeur selon les conditions de l'article « Résiliation » des CGAU :

- Lorsque l'Editeur met en œuvre des changements significatifs dans les accords de sous-traitance de Services TIC qui supportent des Fonctions Critiques ou Importantes malgré l'opposition et les demandes de modification formulées par le Client conformément aux dispositions de l'article « Lieu de réalisation des Services et sous-traitance » des présents Engagements DORA ci-avant ;
- Lorsque l'Editeur met en œuvre des changements significatifs des contrats de sous-traitance de Services TIC qui supportent des Fonctions Critiques ou Importantes avant la fin du délai de notification sans l'approbation explicite du Client prévu à l'article « Lieu de réalisation des Services et sous-traitance » des présents Engagements DORA ci-avant ;
- Lorsque l'Editeur sous-traite un Service TIC qui supporte des Fonctions Critiques ou Importantes sans que cela ne soit explicitement autorisé par le Contrat.

La résiliation interviendra à l'issue du préavis et donne lieu à application de la clause de réversibilité et à l'activation du plan de réversibilité tel qu'indiqué dans les Conditions Générales.

6. FORMATION

L'Editeur s'engage en outre à faire participer son personnel affecté à la fourniture des Services TIC aux programmes de sensibilisation à la sécurité des technologies de l'information et de la communication et aux formations à la résilience opérationnelle numérique qui auront été élaborés par le Client, conformément à l'article 13, paragraphe 6 du Règlement DORA. Le contenu, la fréquence, la durée et le mode de délivrance de ces programmes et formations, ainsi que les publics auxquels ils s'adresseront seront discutés préalablement entre les Parties.

7. REPORTING DES INCIDENTS DE SECURITE

7.1 Notification initiale : l'Editeur notifiera au Client, rapidement après en avoir pris connaissance et au plus tard 24 heures après en avoir pris connaissance pour tout Incident de sécurité Majeur. Cette notification sera faite à l'adresse e-mail spécifique du Client telle qu'indiquée aux Conditions Particulières.

7.2 Notification intermédiaire : Une notification intermédiaire sera assurée par l'Editeur auprès du Client dans les 72 heures après avoir pris connaissance d'un Incident de sécurité Majeur. Cette notification intermédiaire spécifiera au minimum :

- L'heure, la date et le lieu de l'Incident de sécurité, ainsi qu'une description de l'Incident de sécurité Majeur, y compris une description des Données du Client affectées et potentiellement affectées ;
- Les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de fichiers de données à caractère personnel concernées ;
- Une évaluation des conséquences probables de l'Incident de sécurité Majeur pour les Données du Client ; et
- Les mesures prises et/ou à prendre pour atténuer les conséquences de l'Incident de sécurité Majeur.

Si un Incident de sécurité se produit, l'Editeur devra :

- Fournir rapidement toute autre information et l'assistance qui pourront raisonnablement être demandées par le Client afin de se conformer à ses obligations relativement à l'Incident de sécurité en vertu de la loi applicable ;
- Communiquer au Client toute information complémentaire relative à l'Incident de sécurité à laquelle l'Editeur pourrait avoir accès après la notification initiale de l'Incident de sécurité au Client ; et
- Ne pas informer de tiers de l'Incident de sécurité sans le consentement écrit préalable du Client, sauf si l'Editeur est contraint par la loi applicable. Dans ce cas, l'Editeur recueillera l'approbation écrite préalable du Client sur le contenu de cette information afin de minimiser son impact négatif sur ce dernier ;
- Si le Client le demande, effectuer une analyse sur les causes de l'Incident de sécurité et communiquer rapidement au Client les résultats de cette analyse ;
- Déterminer si l'Incident de sécurité est susceptible de se répéter ou est toujours en cours ; et
- Entreprendre des actions immédiates pour éviter que l'Incident de sécurité ne se reproduise.

L'Editeur fournira toute coopération et toute assistance que le Client pourra raisonnablement demander afin d'exercer ses droits relativement à l'Incident sécurité.

8. NIVEAUX DE SERVICE

Lorsque les Services objets du Contrat sont qualifiés par le Client de Services TIC soutenant des Fonctions Critiques ou Importantes, l'Editeur s'engage à :

- Respecter les Niveaux de Service tels que définis au Contrat y compris leurs mises à jour et révisions, assorties d'objectifs de performance quantitatifs et qualitatifs précis dans le cadre des Niveaux de Service convenus, afin de permettre un suivi efficace par le Client des Services TIC, et de prendre, sans retard injustifié, des mesures correctives appropriées lorsque les Niveaux de Service convenus ne sont pas atteints ;
- Mettre en œuvre et de tester des plans d'urgence tel que prévu dans son Plan Continuité d'Activité (PCA) communicable au Client sur simple demande et de mettre en place des mesures, des outils et des politiques de sécurité des Services TIC qui fournissent un niveau approprié de sécurité tels que décrits dans la Plan d'Assurance Sécurité (PAS) communicable sur demande au Client.

9. INFORMATIONS SUR LA SURVENANCE D'EVENEMENTS IMPACTANT LES SERVICES TIC

Lorsque les Services sont qualifiés par le Client comme Services TIC soutenant des Fonctions Critiques ou Importantes, l'Editeur s'engage à notifier au Client, sans retard indu, tout changement susceptible d'avoir une incidence significative sur la capacité de l'Editeur à fournir ces Services TIC qui soutiennent des Fonctions Critiques ou Importantes de

manière efficace conformément aux Niveaux de Service convenus au Contrat.

10. REVERSIBILITE

Les modalités de réversibilité au terme du Contrat sont celles stipulées à l'article 12 des Conditions Spécifiques SAE Certifié Marque NF461. Elles s'appliquent quelle que soit la cause de la cessation du Contrat, y compris en cas de résiliation, insolvabilité, ou cessation des activités de l'Editeur.

Pendant la phase de réversibilité, les Services objet du Contrat sont poursuivis dans les conditions du Contrat. Lorsque les Services sont qualifiés par le Client comme étant des Services TIC soutenant des Fonctions Critiques ou Importantes, les Parties s'engagent à prévoir une stratégie de sortie, en particulier la fixation d'une période de transition adéquate obligatoire :

i) au cours de laquelle l'Editeur continuera à fournir les Services TIC concernés en vue de réduire le risque de perturbation au niveau du Client et d'assurer sa résolution et sa restructuration efficaces ;

ii) qui permet au Client de migrer vers un autre prestataire tiers de services TIC ou de recourir à des solutions en internes adaptées à la complexité du service fourni.

11. TEST DE PENETRATION FONDE SUR LA MENACE

Dans le cas où les Services qualifiés par le Client de Services TIC soutiennent des Fonctions Critiques ou Importantes, l'Editeur pourra participer à tout test de pénétration, sous réserve d'un préavis de dix (10) jours ouvrés. La DSSI de l'Editeur rédigera une lettre d'autorisation de tests qui devra être signée par l'ensemble des parties (Client, Editeur, auditeur). Ces tests seront réalisés aux frais du Client, une fois par an maximum pour une durée n'excédant pas dix (10) jours ouvrés. Ce test sera réalisé par des mandataires agréés par l'Editeur et conformément aux standards définis dans le PAS, et ce, sans interrompre ses Services. Les résultats de ces tests seront communiqués à l'Editeur qui prendra les mesures correctives nécessaires.