ANNEXE

Selon le RGPD art 28

**Instructions documentées du responsable de traitement au sous-traitant.**

# Glossaire

* RGPD : Règlement général sur la protection des données
* RT : Responsable de traitement
* ST : Sous-traitant (au sens RGPD)

# Instructions concernant l’organisation

Contractualisation

* Un contrat comprenant des clauses spécifiques RGPD doit être rédigé entre les sous-traitants et le concessionnaire.
* Une procédure doit être mise en place en cas de fuite de données à caractère personnel.
* Le concessionnaire détruit toutes les données collectées après la fin du contrat avec l’autorité organisatrice ou transmet les données à ce dernier sans en conserver une copie.

# Gestion de la sécurité et continuité d’activité

* Le prestataire doit prendre et documenter des mesures techniques et organisationnelles pour assurer la continuité d’activité du système en cas d’incident, ou la reprise d’activité en cas de sinistre (PCA/PRA).
* Le prestataire assure une veille sécurité. En cas d’alerte grave (attaque virale, faille critique) annoncée par le CERT, le correctif ou à défaut la solution de contournement, doit être appliqué dans le délai le plus court adapté à la criticité de l’application et à son exposition publique.
* Les passages de correctifs doivent être précédés d’une sauvegarde spécifique du système et des données qu’il contient, ainsi que de tests sur un environnement de préproduction.

# Instructions générales

Authentifier les utilisateurs

* Un identifiant (login) unique doit être prévu pour chaque utilisateur.
* Une politique de mot de passe doit être mise en place selon les recommandations de la CNIL ([https://www.cnil.fr/fr/securite-authentifier-les-utilisateurs](http://?))
* Si les outils le permettent, obliger l’utilisateur à changer son mot de passe après réinitialisation.
* Si les outils le permettent, limiter le nombre de tentatives d’accès à un compte.

Gérer les habilitations (autorisations d’accès)

* Des profils d’habilitation doivent être mis en place.
* Un processus de suppression des accès obsolètes doit être mis en place.
* Un processus de revue annuelle des habilitations doit être mis en place.

Tracer les accès et gérer les incidents

* Un système de journalisation doit être mis en place, ou a minima proposé.
* Les équipements de journalisation et les informations doivent être protégés.
* Le concessionnaire informe dans un délai court (48h) le RT concernant une faille de sécurité, et il documente cette violation (selon la déclaration faite à la CNIL).

Sauvegarder

* Une sauvegarde régulière doit être mise en place.
* Les opérations de sauvegardes donnent lieu à un compte-rendu régulier.
* La fiabilité des sauvegardes sera mise à l’épreuve par des tests de restauration, dont les rapports seront communiqués au RT.
* Un exemplaire des sauvegardes doit être conservé dans des locaux physiquement séparés du centre informatique du prestataire hébergeant l’application du donneur d’ordres.

Archiver de manière sécurisée

* Des modalités d’accès spécifiques aux données archivées doivent être mises en place.
* La destruction des archives obsolètes doit être effectuée de manière sécurisée.

Maintenance et destruction des données

* Les interventions de maintenance doivent être enregistrées dans un registre.
* Le responsable de l’organisme doit encadrer les interventions effectuées par des tiers.
* Les données de tout matériel doivent être effacées de manière sécurisée avant mise au rebut.

Sécuriser les échanges et transferts

* Une solution de chiffrement doit être mise en place en cas d’échange ou de transfert.
* Les hébergements de données doivent être sécurisés.
* Les transferts vers les hébergements de données doivent être sécurisés.

Fonctions cryptographiques

* Seules les algorithmes, logiciels ou bibliothèques reconnus doivent être utilisés.
* Les codes secrets et les clés cryptographiques doivent être conservés de manière sécurisée.

# Instructions concernant les infrastructures

Protéger les réseaux informatiques

* Une limitation des flux réseau au strict nécessaire doit être mise en place.
* Les accès distants des appareils informatiques nomades doivent être par un moment sécurisé tel un VPN ou un système de bastion.
* Les protocoles de sécurité les plus élevés doivent être mis en place pour les accès sans-fil (WIFI).

Sécuriser les serveurs

* Les accès aux outils et interfaces d’administration doivent être limités aux seules personnes habilitées.
* Une politique rigoureuse de mot de passe doit être mise en place pour les administrateurs.
* Les mises à jour critiques doivent être installées sans délai.
* Une haute disponibilité des données doit être assuré.
* Des outils d’analyse antivirus doivent être mis en place et mis à jour automatiquement.

Sécuriser les postes de travail

* Une procédure de verrouillage automatique de session doit être mise en place.
* Les logiciels utilisés doivent être mis à jour régulièrement.
* Un antivirus doit être mis en place et régulièrement mis à jour.
* Un pare-feu ou firewall logiciel doit être mis en place.
* L’accord de l’utilisateur doit toujours être recueilli avant toute intervention sur son poste.

Sécuriser l’informatique mobile

* Un moyen de chiffrement des équipements mobiles doit être mis en place.
* Un système de sauvegarde ou de synchronisation doit être mis en place.
* Un code secret pour le déverrouillage doit être mis en place.

# Instructions concernant les développements informatiques

Développements informatiques

* Des paramètres respectueux de la vie privée doivent être mis en place pour les utilisateurs finaux (privacy by design).
* Les zones de commentaires doivent être évitées ou strictement encadrées.
* Les tests de développement doivent se faire avec des jeux de données fictives ou anonymisées.

# Instructions concernant les sites web

Hébergement des sites web

* Les sites doivent être hébergés dans l’Union Européenne et de préférence en France.
* L’outil d’analyse d’audience peut être dispensé de consentement selon les recommandations de la CNIL ([https://www.cnil.fr/fr/solutions-pour-les-cookies-de-mesure-daudience](http://?)), si ce n’est pas le cas il faudra recueillir le consentement de l'internaute avec un système permettant de refuser directement.
* Utiliser un gestionnaire de contenu (CMS) ou un dispositif permettant des mises à jour régulières.

Sécurisations des sites web

* Le protocole TLS (HTTPS) doit être privilégié.
* La mise en œuvre du protocole TLS doit être vérifié régulièrement.
* Une vérification qu’aucun mot de passe ou identifiant ne passe dans les URL doit être faite régulièrement.
* Les accès des utilisateurs doivent correspondre à ce qui est attendu.
* Les accès utilisateurs doivent être contrôlés régulièrement.
* Un bandeau d’information doit être mis en place pour les cookies non nécessaires au service.

Formulaires (newsletter ou contact)

* Un champ de texte doit être mis en place afin d’inclure des mentions d’information selon l’utilisation.
* Une case à cocher (opt-in) doit être mise en place.
* Une procédure simple de désabonnement doit être mise en place.

Informations dédiées aux internautes

* Une page dédiée et accessible dans tout le site doit être mise en place pour :
  + Les mentions légales (selon la LCEN)
  + Une politique de confidentialité (selon le RGPD)
* Un dispositif d’information (bandeau par exemple) doit être mis en place concernant les cookies (ou traceurs).
* Un lien entre les mentions légales et la politique de confidentialité doit être mis en place.
* Les cookies ne seront conservés que pour une durée qui n’excède 13 mois.