

ANNEXE 2 - REFERENTIEL PROTECTION PRIVACY BY DESIGN

Point de Contrôle		Mesure conforme	
1	Finalité : finalité déterminée, explicite et légitime	Finalités connues et énoncées de manière détaillée et compréhensible par les personnes dont les données vont être traitées	<input type="checkbox"/>
		Ne pas aller au-delà des finalités déclarées ou effectuer une nouvelle analyse complète pour tout souhait d'ajout de nouvelle finalité	<input type="checkbox"/>
		Ne permettre de recueillir des données que pour un usage précis et bien défini (éviter par exemple les zones de commentaires libres)	<input type="checkbox"/>
		Ne pas aller à l'encontre de la loi, ni des droits ou des libertés fondamentales des personnes (mesure triviale et générale)	<input type="checkbox"/>

Point de Contrôle		Mesure conforme	
2	Minimisation : réduction des données à celles strictement nécessaires	Données traitées décrite avec précision notamment de l'origine de la collecte, des catégories de personnes concernées et des destinataires	<input type="checkbox"/>
		Veiller à ce que les données à collecter soient pertinentes, adéquates et non excessives c'est-à-dire strictement nécessaires à la finalité déclarée	<input type="checkbox"/>
		Ne permettre l'enregistrement que d'informations personnelles pertinentes et en relation avec la finalité déclarée du traitement	<input type="checkbox"/>
		Ne pas procéder à des traitements d'information qui, du fait de leur nature, de leur portée ou de leurs finalités, excluent des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire (sauf analyse préalable poussée effectuée avec le DPO de l'Amue)	<input type="checkbox"/>
		Éviter de traiter le numéro de sécurité sociale (sauf analyse préalable poussée effectuée avec le DPO de l'Amue)	<input type="checkbox"/>
		Eviter de traiter (sauf analyse préalable poussée effectuée avec le DPO de l'Amue) des informations relatives à des infractions, condamnations, mesures de sûreté, biométriques ou subjectives, ou des données sensibles[1] qu'il est interdit de collecter sauf autorisation ou avis spécifique de la CNIL nécessitant des démarches à anticiper plusieurs mois à l'avance	<input type="checkbox"/>

Point de Contrôle		Mesure conforme	
3	Durées de conservation : durée nécessaire à l'accomplissement des finalités, à défaut d'une autre obligation légale imposant une conservation plus longue	Déterminer les durées de conservation par défaut. Ces durées pourront dans un premier temps être issues du document de référence mis à disposition des équipes de conception sur l'intranet de l'Amue	<input type="checkbox"/>
		Implémenter un mécanisme permettant de basculer les données à caractère personnel de leur archive/base active à leur archive intermédiaire	<input type="checkbox"/>
		Prévoir la possibilité d'appliquer à cette occasion les restrictions d'accès ou d'habilitation qui s'imposeront, ainsi que la possibilité de transférer ces archives intermédiaires aux personnes/services chargés de leur destruction ou de leur archivage définitif	<input type="checkbox"/>
		Paramétrer les durées pour anticiper les évolutions réglementaires/légales ou prendre en compte des situations variées intermédiaires aux personnes/services chargés de leur destruction ou de leur archivage définitif	<input type="checkbox"/>
4	Information : respect du droit à l'information des personnes concernées	Paramétrer l'affichage de mention d'information afin de permettre à l'exploitant de l'outil conçu de fournir un lien Internet vers sa propre mention d'information (ou de personnaliser l'affichage d'une mention type en renseignant les éléments paramétrés)	<input type="checkbox"/>
5	Consentement : obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement	Déterminer lesquels des traitements et des données à caractère personnel à traiter exigent un consentement des personnes concernées en mode opt-in et/ou opt-out	<input type="checkbox"/>
		Prévoir en conséquence du point précédent des mécanismes de recueil de consentement : case à cocher (opt-in) ou à décocher (opt-out), par exemple	<input type="checkbox"/>
6	Droit d'opposition et autres droits entrant dans le cadre des articles 12 à 23 du RGPD : effacement (droit à l'oubli), limitation du traitement, portabilité et gestion post mortem ; respect des droits des personnes concernées	Prévoir des mécanismes de suppression des données à caractère personnel relatives à un traitement donné et à une personne concernée et/ou prévoir des indicateurs/marques/ témoins permettant d'exclure une personne donnée d'un traitement	<input type="checkbox"/>
		Prévoir tout mécanisme facilitant l'exercice des droits d'opposition, effacement (droit à l'oubli), limitation du traitement, portabilité, gestion post mortem, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage)	<input type="checkbox"/>
7	Droit d'accès : respect du droit des personnes concernées d'accéder à leurs données	Prévoir une fonctionnalité d'extraction de l'ensemble des données à caractère personnel d'une personne donnée	<input type="checkbox"/>
		Prévoir les mécanismes facilitant l'exercice du droit d'accès pour les scénarios moins larges	<input type="checkbox"/>
8	Droit de rectification : respect du droit des personnes concernées de corriger leurs données et de les effacer	Permettre la rectification - si justifiée - des données personnelles collectées (mesure triviale)	<input type="checkbox"/>
9	Formalités : définition et accomplissement des formalités préalables applicables au traitement	Effectuer l'analyse du régime juridique et des formalités applicables au traitement en fonction de ses finalités et des catégories de données traitées avec l'aide du DPO, en amont du déploiement du traitement dans les établissements	<input type="checkbox"/>
Point de Contrôle		Mesure conforme	

Point de Contrôle		Mesure conforme	
10	En cas de sous-traitance	Coopérer à l'établissement et au respect des clauses contractuelles de sous-traitance proposées par la CNIL après adaptation aux prestations concernées avec l'aide des DPO	<input type="checkbox"/>
		Pour les besoins de bases de formation ou de tests de masse (tests de performance sur données issues des établissements), le sous-traitant n'est pas autorisé à récupérer les données réelles des bases de production en dépit même d'une « convention de confidentialité » entre l'Amue, le sous-traitant et les établissements exploitant l'application maintenue. Au besoin, le sous-traitant devra fournir aux établissements souhaitant coopérer à la réalisation des tests de masse ou à la constitution de bases de formation, un outil d'anonymisation adapté pouvant être appliqué en toute autonomie par ces établissements eux-mêmes sur leurs propres données avant de les transmettre au sous-traitant via l'Amue sous forme déjà anonymisée.	<input type="checkbox"/>
		Les mécanismes d'anonymisation proposés par le sous-traitant devront être correctement explicités et préalablement évaluables par l'Amue.	<input type="checkbox"/>
		Les mises à jour de la base (ou des bases) de formation ou de tests seront à réaliser par ré-applications successives de l'outil d'anonymisation sur les nouvelles données réelles de en établissement. Le sous-traitant prévoira lorsque nécessaire la mise à jour de l'outil d'anonymisation lui-même en cas de changement de structure, ou en cas de tout autre possible impact de versions évolutives du produit de l'offre SI Amue sur cet outil	<input type="checkbox"/>
		Respecter le principe de protection by design/default à toutes les étapes du cycle de vie du produit de l'offre SI Amue	<input type="checkbox"/>
11	Renseignement fiche traitement	Dans le cadre de prestations de tierce maintenance applicative ou d'intégration, renseigner la fiche de traitement type de l'application maintenue et/ou intégrée (cf. modèle CNIL), fiche devant être adaptée par les DPO des établissement exploitant ladite application	<input type="checkbox"/>
12	Sécurité	Fournir aux établissements exploitant l'offre SI Amue les informations et moyens (liés aux logiciels) de prendre effectivement des mesures en fonction des risques pour garantir l'intégrité, la disponibilité et la confidentialité des données à caractère personnel	<input type="checkbox"/>
13	Etude d'impact sur la vie privée (EIVP/PIA)	En présence de données sensibles, fournir aux établissements exploitant l'offre SI Amue les informations et moyens (liés aux logiciels) de mener correctement le volet gestion des risques de l'étude d'impact sur la vie privée exigée par le règlement	<input type="checkbox"/>