QUESTIONNAIRE PRIVACY BY DESIGN

	QUESTIONS	OUI	NON	AUTRE (N/A, NSP…)
1.	**INFORMATION DES PERSONNES (ARTICLES 12, 13, 14 DU RGPD)**			
1.1.	Les personnes sont préalablement informées de l'identité du responsable de traitement et de celle du DPO, de la finalité du traitement, des catégories de données à caractère personnel concernées et des catégories de destinataires, de la durée de conservation des données ou des critères permettant de la déterminer, etc			
1.2	La solution/outil permet d'apporter une information claire, précise et simple			
1.3	La solution/l'outil permet de configurer des messages d'information d'au moins 1200 caractères.			
1.4	Des mentions d'information peuvent être insérées avec différents niveaux de lecture/détails. Pop-up, …			
1.5	Les personnes sont préalablement informées de tout transfert à destination d'un État non membre de l'UE (ou d'une organisation internationale).			
1.6	Les personnes sont préalablement informées de leur droits « Informatique et libertés » applicables au traitement (droits accès, de rectification, d'effacement et de portabilité des données, droits d'opposition et de limitation du traitement des personnes, droit de définir des directives sur le sort de leurs données après leur décès), ainsi que des modalités d'exercice de ces droits			
1.7	Les personnes sont préalablement informées de leur droit de définir des directives sur le sort de leurs données après leur décès (article 85 loi « Informatique et libertés »)			
1.8	Les personnes sont préalablement informées des mécanismes ou techniques utilisés, notamment les mécanismes de chiffrement			
2.	**CONSENTEMENT (LE CAS ECHEANT)**			
2.1	La solution/l'outil permet de recueillir le consentement de la personne et de l'enregistrer			
2.1.1	Le consentement de la personne peut être documenté et prouvé à tout moment.			

2.1.2	Le consentement de la personne peut être révoqué à tout moment, par un moyen simple et par voie électronique, aussi simplement qu'il a été recueilli			
3.	**DUREE DE CONSERVATION**			
3.1	Une fonction paramétrable permet d'alerter l'utilisateur de la solution/outil que les données arrivent à la fin de leur « durée de conservation »			
3.2	Un processus d'archivage a été prévu. Individuellement ou massivement (requêtes paramétrables)			
3.34	Il existe un moyen simple de supprimer les données, individuellement ou massivement (requêtes paramétrables) – effacement logique			
4	**EFFACEMENT PHYSIQUE DES DONNEES ET DES METADONNEES**			
4.1	• sans délai pour les espaces de stockage courants et les éventuelles copies répliquées en ligne (synchronisées en temps réel ou en miroir) ; • dans un délai maximum d'un mois pour les sauvegardes (incrémentales, complètes… réalisées à fréquence donnée).			
5	**DROITS DES PERSONNES :** **DROITS D'ACCES, DE RECTIFICATION, D'EFFACEMENT DES DONNEES (ARTICLES 15, 16, 17, DU RGPD)**			
5.1.	Un processus permet de répondre à une demande d'exercice de droit d'accès aux données dans le délai de réponse prévu			
5.2.	Un processus permet de répondre à une demande d'exercice de droit de rectification des données dans le délai de réponse prévu			
5.3.	Un processus permet de répondre à une demande d'exercice de droit à l''effacement des données dans le délai de réponse prévu			
	DROITS DES PERSONNES : **DROIT A LA LIMITATION AU TRAITEMENT, DROIT D'OPPOSITION AU TRAITEMENT (ARTICLES 18 ET 20 DU RGPD)**			
	Un processus permet de répondre à une demande d'exercice de droit à la limitation du traitement (gel temporaire du traitement)			
	Un processus permet de répondre à une demande d'exercice de droit d'opposition au traitement			
	Décisions individuelles automatisées (article 22 du RGPD)			
	Un processus permet de répondre à un droit d'opposition d'une personne à une décision individuelle automatisée (décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire)			
	Un processus permet de répondre à une demande d'une personne d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision automatisée			

6	**DROITS DES PERSONNES :** **DROIT A LA PORTABILITE (ARTICLE 20 DU RGPD**			
6.1	Possibilité de récupérer l'intégralité des données sur une personne de façon simple, sans manipulation complexe ou répétitive, et dans un format électronique structuré et couramment utilisé, afin de faciliter le changement de fournisseur, et ce sans collecter d'informations confidentielles (telles que les identifiants bancaires, les mots de passe de service en ligne, etc.).			
	Catégories de données particulières/sensibles (articles 9 et 10 du RGPD)			
	Des règles renforcées de protection et de sécurité relatives au traitement des données sensibles sont prévues (origine ethnique ou raciale, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, santé, vie et orientation sexuelle, données génétiques, données biométriques d'identification d'une personne unique)			
	Des règles renforcées de protection et de sécurité relatives au traitement des données relatives aux condamnations, infractions pénales et mesures de sûreté connexes sont prévues			
	Zones « commentaires libres »			
	Si des zones de « commentaire libre » ou « bloc-notes » sont prévues, un dispositif permet d'éviter la saisie de commentaires "à risque" (dérouleur ou blocage de certains mots ou pop-up d'avertissement ou de consignes)			
7	**OBLIGATIONS GENERALES (ARTICLE 24 DU RGPD)** **POSSIBILITE DE METTRE EN PLACE DES MESURES ORGANISATIONNELLES VISANT A PROTEGER LES DONNEES.**			
7.1	Authentification			
7.1.1	Authentification, définition de rôles avec différents niveaux d'accès aux données			
7.1.2	Le service numérique ne permet de s'authentifier que par des mécanismes d'authentification robustes (mots de passe à usage unique, envoi de codes par SMS…).			
7.1.3	La clé d'identification n'est pas le numéro de sécurité sociale (NIR)			
8	**SECURITE DES DONNEES**			
	Des standards ou des guides de bonnes pratiques de sécurité sont appliqués (ISO 27001, ISO 27018, ISO 2000-1, guide d'hygiène et kit de sécurité ANSSI, guide sécurité CNIL…)			

	Une politique/procédure d'habilitation d'accès au traitement est prévue (critères d'attribution, revue annuelle, suppression des permissions d'accès obsolètes…)			
8.1	Le service numérique intègre des outils permettant de bloquer des connexions faites par des robots et de retarder et/ou de bloquer les connexions illégitimes faites par des personnes.			
8.2	Le service numérique intègre des mesures visant à garantir l'intégrité et la disponibilité des données (centre de stockage redondant, sauvegardes régulières…).			
	Des tests d'intrusions ont été effectués (depuis l'extérieur en mode « boite noire », en interne, sur les accès Wifi…)			
	Un dispositif permet de détecter et prévenir les incidents impactant la disponibilité, la confidentialité ou l'intégrité des données, et en cas d'incident, de les rétablir dans des délais appropriés			
	Un mécanisme de traçabilité/journalisation des activités sur le traitement est prévu			
9	**ANONYMISATION, PSEUDONYMISATION ET CHIFFREMENT**			
9.1	Le service numérique intègre une fonction d'anonymisation des données conservées, incluant les documents stockés et leurs métadonnées			
	Le service numérique intègre une fonction de pseudonymisation des données conservées, incluant les documents stockés et leurs métadonnées			
	Le service numérique intègre une fonction de chiffrement / déchiffrement des données conservées, incluant les documents stockés et leurs métadonnées			
10	**GEOLOCALISATION**			
10.1	Le dispositif peut être désactivé à tout moment.			
11	**HEBERGEMENT DES DONNEES PAR LE FOURNISSEUR DE SERVICE**			
11.1	Le fournisseur propose des mesures techniques et organisationnelles permettant d'empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations)			
11.2	Le fournisseur propose des mesures techniques et organisationnelles permettant d'empêcher que les supports de données puissent être lus, copiés, modifiés ou supprimer de façon non autorisée (contrôle des supports de données)			
11.3	Le fournisseur propose des mesures techniques et organisationnelles permettant d'empêcher l'introduction non autorisée de données à			

	caractère personnel dans le ficher, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de conservation)			
12	**TRANSFERTS DE DONNEES EN-DEHORS DE L'UE**			
12.1	Le fournisseur est en capacité de démontrer qu'aucun transfert de données en dehors de l'UE n'est réalisé (définition d'un transfert : communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quel que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire)			
12.2	Le fournisseur est en capacité de démontrer que toutes les données sont stockées et sauvegardées dans l'UE.			
	Si un transfert de données a lieu vers un pays tiers à l'UE, le fournisseur est en mesure d'indiquer vers quel(s) pays			
	Si un transfert de données a lieu vers un pays tiers à l'UE, le fournisseur est en mesure de démontrer qu'une décision d'adéquation a été prise par la Commission européenne			
	A défaut de décision d'adéquation, le fournisseur est en mesure de démontrer qu'une « garantie appropriée » prévue par le RGPD a été mise en œuvre (BCR/règles d'entreprise contraignantes, « clauses contractuelles types » adoptées par la Commission européenne, code de conduite, etc)			