PRIVACY BY DESIGN

Le document liste à titre indicatif les questions à se poser sur les fonctionnalités du logiciel, de l’application, du fichier de traitement de données à caractère personnel, en vue de déterminer s’il respecte les principes de Privacy by Design, Privacy by reDesign et Privacy by Default (cf art. 25 du RGPD).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **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** |  |  |  |
| 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.** | **Durée 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 données et des métadonnées** |  |  |  |
| 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'accès, de rectification, d’effacement des données** *(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 à 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 à la portabilité** *(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 générales** *(article 24 du RGPD)*  Possibilité de mettre en place des mesures organisationnelles visant à protéger les données. |  |  |  |
| **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** | **Sécurité des données** |  |  |  |
|  | 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** | **Géolocalisation** |  |  |  |
| 10.1 | Le dispositif peut être désactivé à tout moment. |  |  |  |
| **11** | **Hébergement des données 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 données 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) |  |  |  |

**ANNEXE 2 Quelques exemples concrets de mesures techniques et organisationnelles de « Privacy by (re) Design / Privacy by Default »**

Toujours impliquer le DPO (et en garder trace) en amont de la création ou mise à jour d'un nouveau projet de service, logiciel, fichier, application, etc. (projet de traitement).

Exemples de mesures organisationnelles : rédaction de politique (ex : politique de conservation et de suppression des données, politique d’habilitation, politique de gestion des incidents liés aux systèmes d’information  procédures, chartes, suppression de données non pertinentes ou interdites, définition et mesures d’audit, signature de clauses contractuelles contraignantes dans les contrats de sous-traitance, sensibilisation du personnel aux enjeux de sécurité et de confidentialité des données (sessions de formation, rédaction de notes de services)…

Mettre en place des mesures techniques visant à empêcher l’accès non autorisé aux données, la modification ou la disparition des données ainsi que l’indisponibilité des données.

Exemples de mesures techniques de sécurité : contrôle des accès, mécanisme d’authentification, mesures de traçabilité, sauvegardes, déclenchement et analyse de tests d’intrusion.

Développer des mécanismes d’anonymisation, de pseudonymisation ou de chiffrement.

Chiffrement : TLS devrait être employé pour l’utilisation du protocole https.

Le traitement doit permettre de ne collecter que les données dont le responsable de traitement a *réellement* besoin et non pas parce que « cela peut servir » (minimisation de la collecte des données).

A chaque évolution du traitement, initier une procédure de révision de la pertinence des données collectées pour signaler, au moyen d’une icône, les données qui ne sont plus absolument nécessaires.

Toujours vérifier si pour le traitement, le lien entre les données traitées et les personnes physiques est indispensable.

Intégrer une fonctionnalité permettant de lister toutes les données à caractère personnel d'une personne physique pour faciliter le travail de recherche des données et la réponse à une demande de droit d'accès. La fonctionnalité doit permettre de distinguer d'une part les données actives et d'autre par les données en archives intermédiaires.

Intégrer dans tout développement de logiciel la notion d'archives intermédiaires avec une gestion des droits qui permette de restreindre les accès à ces archives intermédiaires.

Pour permettre le respect du droit à la limitation du traitement, intégrer une fonction « verrouillage » pour s'assurer que pendant toute la durée de la limitation, les données ne pourront pas être exploitées.

Identifier les données soumises à portabilité et définir un format « structuré couramment utilisé et lisible par une machine » permettant d’automatiser leur transmission (système permettant un export exploitable pour la portabilité).

Prévoir un système d’accusé de réception lorsque les demandes d’exercice de droits (droit d’accès, droit de rectification, etc) est effectuée directement sur le système par la personne concernée.

Une durée de conservation pour chaque catégorie de donnée doit être fixée en tenant compte de ce qui est strictement nécessaire au bon fonctionnement du service. Pour que la procédure d’effacement soit efficace, le développeur doit distinguer entre les données présentes dans ses serveurs, celles présentes dans les serveurs de son sous-traitant et celles traitées en local dans le moniteur et le téléphone de l’utilisateur.

Intégrer un processus de destruction automatique et systématique des données une fois leur finalité « épuisée » (purge automatique) et prévoir aussi une fonction de purge manuelle.

Chaque modification devrait être horodatée et la date de dernière modification conservée dans l’application pour être vérifiée à la reconnexion. En cas de différence l’utilisateur recevrait une alerte.