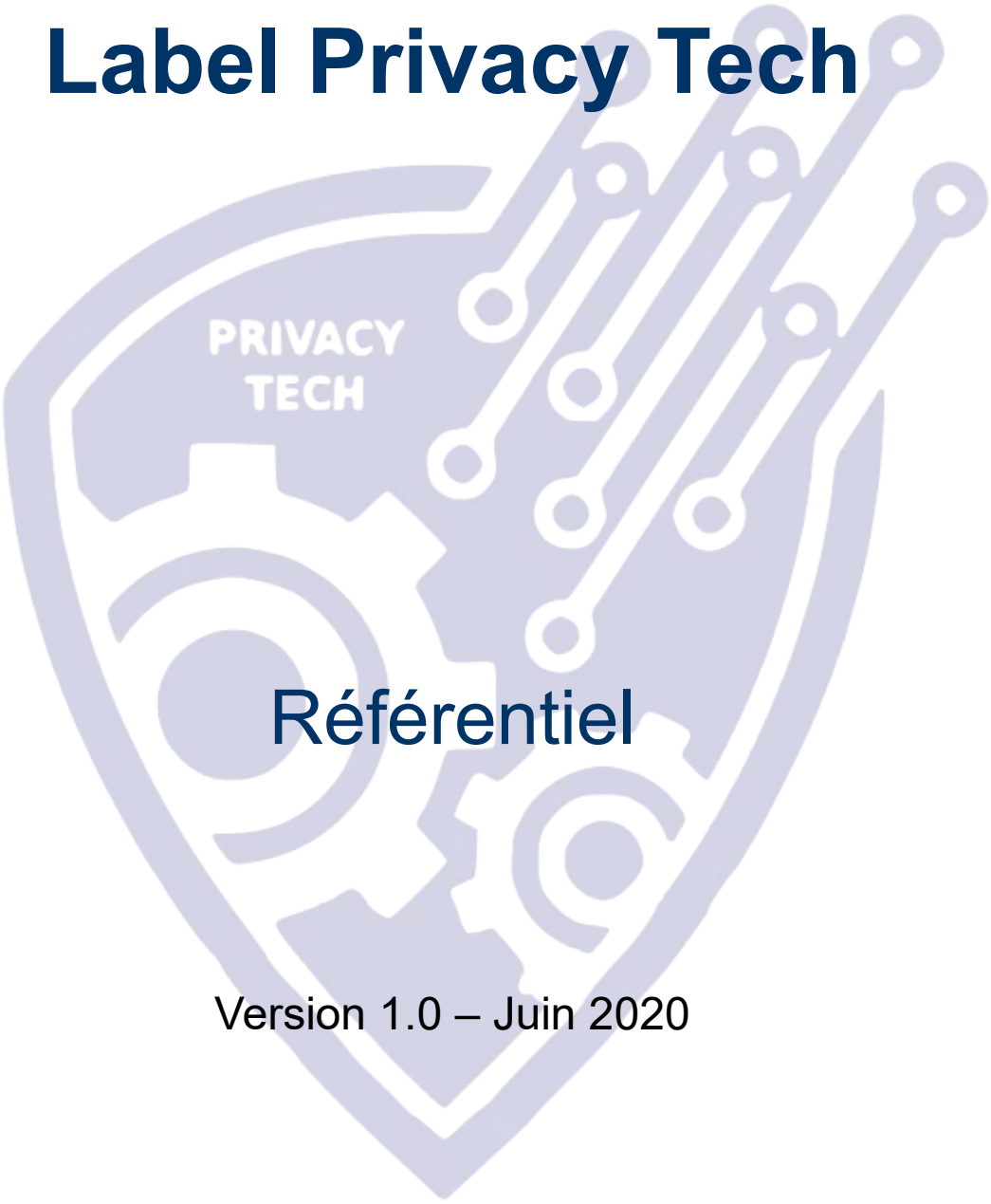
Label Privacy Tech



Référentiel

Version 1.0 – Juin 2020

Table des matières

I. Introduction

1. L'Association Privacy Tech

PRIVACY TECH est une association qui poursuit depuis sa création un projet d'innovation collaborative destiné à recenser, à promouvoir et à co-développer des solutions juridico-techniques au service de la protection de la vie privée sur Internet.

Pour l'Association Privacy Tech, stimuler l'excellence française en matière de « Privacy » est un objectif à atteindre.

2. Génèse du « Label Privacy Tech »

a. Un constat: le marché a besoin d'un label, gage de confiance et outil de valorisation

L'entrée en application du Règlement Général sur la Protection des Données le 25 mai 2018, a donné naissance à une myriade de vocation pour la protection des données à caractère personnel. En effet de nombreux "apprentis-experts RGPD" s'improvisent sur ce marché et profitent de l'épée de Damoclès que représentent les nouvelles sanctions en proposant du conseil, de la formation ou encore des solutions logicielles miracles pour se mettre en conformité.

Les Responsables de traitement, qui sont très prudents dans le choix des outils dédiés à la mise en conformité au RGPD, ont des difficultés à faire la part des choses devant l'étendue des solutions disponibles.

Dans ce contexte il est souvent très compliqué pour les « start-up » passionnées d'atteindre la signature du contrat. En effet la mise en concurrence est rude et les périodes d'avant-vente ou de réponse aux appels-offres sont chronophages et coûteuses pour ces jeunes entreprises.

Comment permettre à cet écosystème français de passer ses frontières en fluidifiant leurs négociations et assurer un facteur confiance à la hauteur des attentes des organismes de toutes tailles ?

Une réponse à cette question est le « Label Privacy Tech ».

b. L'élaboration du label

Afin d'avoir une vision sur les différents types de solutions sur le marché l'Association Privacy Tech a participé à l'organisation de la Trust&Privacy Night 2018 en collaboration avec U Change (créateur des Trust&Privacy Day 2016 et 2017), SNCF développement et K&L Gates. La Trust&Privacy Night regroupa le 25 avril 2018, 350 professionnels directement concernés par la mise en conformité RGPD : startups, PME, ETI et grandes entreprises.

Toutes les startups sélectionnées ont présenté en quelques minutes leurs solutions avec un focus sur leur capacité à apporter une solution concrète dans le cadre de l'application du Règlement Général sur la Protection des Données.

Cet événement a permis de mettre en lumière les fonctionnalités communes aux solutions logicielles de mise en conformité au RGPD les plus exigeantes et ainsi de pré-sélectionner des exigences à respecter dans le cadre d'un label.

À la suite de cet événement, le bureau de l'Association Privacy Tech s'est réuni pour acter le projet de créer un référentiel de labellisation afin d'initier un groupe de travail avec AFNOR Certification.

3. Les 5 catégories de solutions logicielles concernées par le « Label Privacy Tech »

Les solutions logicielles sont classées en catégories en fonction de leurs fonctionnalités. Les exigences applicables dans le cadre du « Label Privacy Tech » vont varier en fonction des catégories.

Les différentes catégories de solution sont les suivantes :

Catégorie 1.

Data Protection Management Asset : cette catégorie regroupe toutes les solutions logicielles qui permettent à un organisme de répondre à un ou plusieurs principes fondamentaux assurant la licéité des traitements (Droit d'information, garanties de l'exercice des droits, gestion des consentements etc..).

Catégorie 2.

Data Protection Management Solution : cette catégorie regroupe toutes les solutions logicielles qui permettent à un organisme de répondre à ses obligations documentaires (Registre, PIA, registre d'exercice des droits, journal des violations).

Catégorie 3.

Data Processor Compliant Solution : cette catégorie regroupe toutes les solutions logicielles mises à disposition par un organisme qui a vocation à endosser un rôle de sous-traitant au sens du RGPD (solution logicielle RH, solution logicielle CRM, solution logicielle d'archivage, plateforme de gestion d'évènements, plateforme de routage courriel …).

Catégorie 4.

Personal Data Management : cette catégorie regroupe toutes les solutions logicielles tournées sur l'individu qui renforcent l'autodétermination informationnelle par la maîtrise et le contrôle par l'utilisateur sur ses données personnelles.

Catégorie 5.

Sovereign Solution : cette catégorie regroupe toutes les solutions souveraines à destination de personnes physiques répondant à des besoins aujourd'hui majoritairement couverts par les services de la société de l'information (Moteurs de recherche, messageries électroniques, réseaux sociaux, plateformes, newsletters, etc.)

II. Processus de labellisation

1. Candidature au « Label Privacy Tech »

a. Champ d'application du label

Le « Label Privacy Tech » est destiné aux solutions logicielles appartenant aux cinq catégories définies au chapitre 3 de l'Introduction :

- Catégorie 1 : Data Protection Management Asset
- Catégorie 2 : Data Protection Management Solution
- Catégorie 3 : Data Processor Compliant Solution
- Catégorie 4 : Personal Data Management
- Catégorie 5 : Sovereign Solution

Le label est attribué à une solution logicielle. Un organisme (privé ou public) éditant plusieurs solutions logicielles et souhaitant obtenir le label pour chacune d'elles devra candidater séparément et présenter un dossier complet pour chaque solution.

L'organisme d'évaluation tierce partie assure, en liaison avec l'Association Privacy Tech, la gestion de la labellisation depuis la réception du dossier de candidature complet jusqu'à la délivrance du rapport et de sa synthèse.

b. Demande de labellisation

Le candidat à la labellisation pour sa solution logicielle se connecte à la plateforme logicielle d'évaluation du label gérée par l'organisme d'évaluation et crée un compte en renseignant des informations relatives à son identification et aux échanges d'informations. Après validation de son compte par l'organisme d'évaluation, le candidat pourra avoir accès à l'espace prévu pour son évaluation.

2. Phase initiale de labellisation

La labellisation d'une solution logicielle intervient à l'issue d'une procédure d'examen menée par un organisme d'évaluation tiers et indépendant de l'Association Privacy Tech, en trois étapes, et selon les conditions suivantes :

- Constitution et dépôt du dossier de candidature par l'organisme candidat éditeur ou fournisseur de la solution logicielle ;
- Évaluation du dossier de candidature par un évaluateur sous la responsabilité d'un organisme d'évaluation tiers indépendant ;
- Au regard du rapport d'évaluation transmis par l'évaluateur, décision motivée de celui-ci portant délivrance du label ou de refus de labellisation au nom de l'Association Privacy Tech.

a. Constitution du dossier des preuves documentaires

Les critères d'évaluation et les éléments documentaires de preuves associées à collecter par le candidat sont définis au chapitre III du présent référentiel. Ceux-ci devront être téléversés dans la plateforme logicielle d'évaluation de l'organisme d'évaluation afin d'être analysés par un évaluateur missionné pour l'occasion.

Après avoir téléversé toutes les preuves documentaires nécessaires pour attester du respect des exigences du label, l'organisme candidat notifie par l'intermédiaire de la plateforme logicielle d'évaluation à l'organisme d'évaluation la complétude de son dossier et demande à ce qu'il soit évalué. Une facture liée à l'évaluation est alors générée automatiquement et transmise au candidat.

Après validation de son compte sur la plateforme logicielle par l'organisme d'évaluation, l'organisme candidat dispose d'un délai maximum de trois mois pour constituer son dossier et demander à ce qu'il soit évalué. Passé ce délai le dossier sera clôturé si aucune demande d'évaluation n'a été faite par l'organisme candidat.

b. Évaluation par l'organisme d'évaluation

L'évaluation a pour but d'apprécier à distance la conformité des pratiques mises en œuvre par l'organisme candidat au regard des exigences du « Label Privacy Tech » dans sa version en vigueur. Cette phase d'évaluation à distance est réalisée par l'organisme d'évaluation.

Un évaluateur missionné par l'organisme d'évaluation procède à l'analyse du dossier de candidature à la labellisation ainsi que des éléments documentaires attestant du respect des critères d'évaluation qui auront été préalablement demandés à l'organisme candidat.

Cette analyse peut donner lieu à une et une seule demande d'informations et/ou de documents complémentaires. Dans le cas où l'évaluateur adresse une demande de précisions complémentaires ou de documents complémentaires, le candidat dispose d'un délai maximal de deux semaines pour y répondre. En l'absence de réponse du candidat dans le délai imparti, l'évaluation se poursuivra et le rapport sera finalisé au vu du dossier initial déposé par le candidat.

Le rapport d'évaluation est adressé au candidat, incluant les commentaires de l'évaluateur ainsi que la décision de labellisation découlant de l'analyse de l'évaluateur.

À titre indicatif, le délai de traitement d'un dossier entre la demande faite par le candidat et la fourniture du rapport d'évaluation par l'organisme d'évaluation est d'un à deux mois sous réserve de la complétude du dossier.

3. Labellisation

a. La décision de labellisation

L'Association Privacy Tech est seule responsable de l'attribution ou du refus d'attribution du « Label Privacy Tech ». La décision prononcée par l'évaluateur représentant l'organisme d'évaluation dans le rapport d'évaluation est validée automatiquement par l'Association Privacy Tech. Cette décision, quel qu'en soit le sens (attribution du label ou refus), est motivée et notifiée au candidat par l'organisme d'évaluation.

b. Délivrance d'une attestation de labellisation

La labellisation est matérialisée par la délivrance d'une attestation de labellisation, c'est à dire un document officiel délivré par l'organisme d'évaluation au nom de l'Association Privacy Tech attestant la conformité aux exigences du référentiel du « Label Privacy Tech ».

L'attestation doit notamment permettre d'identifier la solution logicielle labellisée avec au minimum :

- le nom de la solution logicielle labellisée ;
- la catégorie (parmi les 5) à laquelle appartient la solution logicielle labellisée ;
- le nom et l'adresse de l'organisme candidat éditeur ou fournisseur de la solution logicielle ;
- la date d'effet et la période de validité.

Cette attestation de labellisation est valable pour une durée de trois ans à partir de la date de décision de labellisation.

La liste des organismes labellisés sera disponible sur l'espace dédié au « Label Privacy Tech » sur le site internet de l'organisme d'évaluation.

c. Utilisation de la marque

Pour faire valoir sa labellisation et dès lors qu'il est titulaire d'une attestation de labellisation en cours de validité, l'organisme labellisé est en droit d'utiliser la marque collective afférente à la catégorie du « Label Privacy Tech » concernée par sa solution logicielle dans les conditions précisées contractuellement et le respect des principes de clarté et de sincérité.

L'organisme candidat ne doit pas communiquer sur son « Label Privacy Tech » pour d'autres solutions que celles ayant fait l'objet de l'évaluation et dont le label lui a été délivré

L'organisme candidat doit s'abstenir d'exercer une activité promotionnelle (publicité, matériel d'information, etc.) qui pourrait conduire ses clients ou prospects à une interprétation inexacte de la signification du « Label Privacy Tech ».

d. Conditions de suspension et de retrait de la labellisation

Une décision de suspension de la labellisation peut être prise à l'égard d'une solution logicielle labellisée :

- à la demande de l'organisme candidat éditeur ou fournisseur de la solution labellisée, notamment en cas d'évolution technique majeure/nouvelle version empêchant momentanément le maintien de la conformité de sa solution aux exigences du présent référentiel ;
- à l'initiative de l'organisme d'évaluation au nom de l'Association Privacy Tech, en raison de non-conformités constatées par rapport au référentiel à la suite d'une évaluation de renouvellement du label ou d'une évaluation ponctuelle en cours du cycle de labellisation ;
- à l'initiative du Comité de labellisation, à la suite d'une plainte d'un utilisateur de la solution labellisée (client de l'organisme candidat) auprès de l'organisme d'évaluation. Dans cette hypothèse, l'organisme d'évaluation engage une discussion avec l'organisme candidat sur le bien-fondé de la plainte du client et les mesures à prendre. Si un désaccord entre l'organisme candidat et l'organisme d'évaluation persiste sur la caractérisation de l'incident et les mesures préconisées, l'organisme d'évaluation soumet la difficulté au Comité de labellisation qui pourra décider après analyse de suspendre la labellisation.

La suspension entraîne le retrait provisoire de l'entreprise de la liste des organismes labellisés publiée sur le site de l'organisme d'évaluation, pendant la période de suspension déterminée. Pendant toute la durée de suspension, l'entreprise concernée ne peut plus se prévaloir du label, ni dans ses relations commerciales avec ses clients, ni dans ses publications commerciales et ses supports de communication.

Le fait pour l'entreprise concernée de continuer à se prévaloir de quelque manière que ce soit du « Label Privacy Tech » pendant la période de suspension entraînera le retrait du label.

Le délai maximum de suspension du « Label Privacy Tech » est de 6 mois.

Après analyse de nouveaux éléments transmis par l'organisme candidat labellisée, la levée de la suspension, le maintien de la suspension ou le retrait de la labellisation peuvent être décidés.

Toute partie prenante peut adresser à tout moment à l'organisme d'évaluation les éléments dont elle a connaissance et qui sont susceptibles de caractériser une violation des prescriptions des exigences et critères du label. L'organisme d'évaluation procédera à leur instruction de manière strictement confidentielle.

e. Devoir de transparence

L'organisme candidat informe l'organisme d'évaluation de toute situation nouvelle susceptible d'affecter son label, notamment concernant son identité ou son statut, ses effectifs, son organisation, son activité, son système de management, ses services, les personnes ayant pouvoir de décision ou leur(s) représentant(s), les évolutions techniques majeures de la solution labellisée. L'Association Privacy Tech peut évaluer l'incidence de ces modifications sur le maintien de la labellisation.

f. Evaluations ponctuelles

Des évaluations ponctuelles peuvent intervenir à tout moment au cours du cycle de labellisation et en sus, dès lors que l'Association Privacy Tech, le Comité de labellisation ou l'organisme d'évaluation possèdent des éléments crédibles de nature à remettre en cause l'attribution du label. Dans ce cas, le Comité de labellisation est consulté pour l'évaluation à mener pour valider le maintien du label. Seul le Comité de labellisation peut prendre la décision de mener une évaluation ponctuelle en cours de cycle. Cette éventuelle évaluation ponctuelle sera à la charge de l'entreprise concernée. À l'issue de l'évaluation de vérification, le Comité de labellisation pourra décider, soit le maintien, soit la suspension de la labellisation, soit le retrait de la labellisation.

Dans le cas où l'organisme candidat en cause refuse la mise en œuvre d'une évaluation ponctuelle, le Comité de labellisation pourra prononcer une décision de suspension ou retrait du label s'il estime que la conformité aux exigences du label de la solution logicielle de l'organisme candidat en cause n'est plus assurée au regard des éléments dont il dispose.

4. Renouvellement

a. Préparation du renouvellement de la labellisation

Six mois avant l'échéance de l'attestation « Label Privacy Tech », l'organisme d'évaluation informe l'organisme candidat éditeur ou fournisseur de la solution labellisée des dates d'échéances. Elle lui communique les dispositions nécessaires à engager pour le renouvellement du « Label Privacy Tech ».

Le renouvellement permet d'engager un nouveau cycle de labellisation de trois ans dans les mêmes conditions que le cycle initial afin d'assurer que la solution logicielle labellisée continue de satisfaire aux critères de labellisation.

b. Décision de renouvellement de la labellisation

Au moins 1 mois avant l'expiration de la durée de validité du label, la solution logicielle fait l'objet d'une évaluation de renouvellement menée par l'organisme d'évaluation. Cette évaluation donne lieu à la rédaction d'un rapport d'évaluation motivé aboutissant à la décision suivante :

- soit le renouvellement du label ;
- soit la suspension du label assorti de demandes de mise en conformité ;
- soit le retrait motivé du label.

L'organisme d'évaluation notifie sa décision motivée à l'organisme candidat.

Sauf cas d'urgence, la suspension ou le retrait du label ne peuvent intervenir qu'après avoir informé l'organisme candidat de la mesure envisagée et l'avoir mis à même de présenter ses observations.

5. Comité de labellisation

a. Constitution du comité

Le Comité de labellisation est constitué et animé par l'Association Privacy Tech qui en assure le secrétariat.

Il est composé de 3 collèges d'experts différents :

- Organisme d'évaluation : entre 1 et 2 représentants
- Editeurs labellisés : entre 1 et 3 représentants
- Association Privacy Tech : entre 1 et 3 représentants

b. Missions du comité

Le comité se réunit physiquement au moins une fois par an pour :

- traiter les plaintes et réclamations pour lesquelles un désaccord subsiste entre l'organisme d'évaluation et le plaignant après que l'organisme d'évaluation ait traité celles-ci ;
- traiter les plaintes et réclamations pour lesquelles l'organisme d'évaluation sollicite l'avis du comité ;
- pour discuter des futurs développements et améliorations ;
- pour réviser le présent référentiel au besoin.

Afin d'éviter tout conflit d'intérêt, tout représentant faisant partie d'un organisme concerné par une réclamation sera amené à ne pas siéger lors de l'examen de ce dossier en comité. De manière générale les membres du Comité de labellisation devront signaler tout conflit d'intérêt éventuel au regard des entreprises dont les dossiers sont examinés.

Tout avis du comité de labellisation doit être motivé.

III. Exigences du « Label Privacy Tech »

Ces exigences visent à labelliser les cinq catégories de solutions logicielles. Les exigences à appliquer varient en fonction des catégories.

1. Conditions préalables à remplir par l'organisme candidat présentant une solution à la labellisation

Exigence 1.1 :

Pour pouvoir accéder à la phase d'évaluation, l'organisme candidat remplit toutes les conditions préalables suivantes :

- Justifier de la désignation d'un délégué à la protection des données (DPO) par l'organisme.
- Justifier de l'adhésion à l'association PRIVACY TECH

Éléments d'auditabilité :

- Téléversement du récépissé de désignation auprès de la CNIL.
- Téléversement de l'attestation émise par Privacy Tech

L'exigence 1.1 est imposée aux cinq catégories.

2. Exigences liées à l'organisme

Exigence 2.1 :

L'organisme possède une politique ou des règles internes en matière de protection des données.

Eléments d'auditabilité :

- Téléversement de la politique de protection des données interne à l'organisme.

L'exigence 2.1 est imposée aux cinq catégories.

Exigence 2.2 :

L'organisme met en œuvre des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement que sa solution logicielle assure.

Eléments d'auditabilité :

- Téléversement du Plan d'Assurance Sécurité (PAS) lié à la solution logicielle évaluée

L'exigence 2.2 est imposée aux cinq catégories.

Exigence 2.3 :

L'organisme met en œuvre des mesures de protection des données dès la conception et/ou par défaut adaptées aux risques et à la nature des opérations de traitement que sa solution logicielle assure telles que le chiffrement ou un système assurant le principe de minimisation sur les différents points de collecte que la solution logicielle peut assurer.

Eléments d'auditabilité **:**

- Téléversement d'une déclaration du DPO qui acte le fait qu'une réelle étude sur le principe de minimisation a été conduite sur l'ensemble des interfaces ou des points de collecte de la solution.

L'exigence 2.3 est imposée aux cinq catégories.

Exigence 2.4 :

L'organisme tient à jour le registre des activités de traitement ainsi que la documentation nécessaire pour prouver la conformité à la réglementation en matière de protection des données pour les traitements que sa solution logicielle assure à ses clients.

Eléments d'auditabilité :

- Téléversement des fiches de traitement liées à la solution pour répondre aux exigences de l'article 30.2 du RGPD

L'exigence 2.4 est imposée aux trois premières catégories.

Exigence 2.5 :

L'organisme respecte le cadre juridique relatif à la sous-traitance en matière de traitement de données à caractère personnel et a fortiori l'ensemble des obligations de l'article 28 du Règlement Général sur la Protection des Données (RGPD).

Eléments d'auditabilité :

- Téléversement des clauses contractuelles de sous-traitance.

L'exigence 2.5 est imposée aux trois premières catégories.

Exigence 2.6 :

L'organisme informe ses clients ou utilisateurs concernant les instruments juridiques susceptibles d'être utilisés si des transferts de données hors Union européenne existent dans un ou plusieurs des processus qu'il assure.

Eléments d'auditabilité :

- Téléversement des mentions d'information avec l'url de ces dernières ou téléversement d'une attestation du DPO dans le cas où il n'y a pas de flux hors UE

L'exigence 2.6 est imposée aux cinq catégories.

Exigence 2.7 :

L'organisme sait accompagner ses clients en matière d'analyse d'impact relative à la protection des données (en particulier si l'un ou plusieurs processus d'un traitement de données à caractère personnel sont assurés par le biais de la solution évaluée). Il est en mesure d'assurer la reddition de comptes nécessaire pour les différentes mesures techniques et organisationnelles qu'il assure pour ses clients dans le cadre de la solution logicielle.

Eléments d'auditabilité :

- Téléversement du Plan d'Assurance Sécurité (PAS) lié à la solution logicielle évaluée.

L'exigence 2.7 est imposée aux trois premières catégories.

Exigence 2.8 :

L'organisme informe de toutes vulnérabilités détectées dans sa solution logicielle susceptible d'engendrer une violation de données personnelles nécessitant une notification à l'autorité de contrôle et/ou une communication aux personnes concernées.

Eléments d'auditabilité :

- Téléversement de la procédure formalisée liée à ce type d'événement
- Téléversement des « printscreen » des interfaces dédiées à la journalisation de ces évènements (uniquement pour la seconde catégorie)

L'exigence 2.8 est imposée aux cinq catégories.

Exigence 2.9 :

L'organisme autorise la réalisation d'audit, par une tierce partie, en matière de protection des données à la demande et aux frais de ses clients.

Eléments d'auditabilité :

- Téléversement de l'engagement contracté avec le Responsable de traitement.

L'exigence 2.9 est imposée aux trois premières catégories.

3. Exigences liées à la solution :

Exigence 3.1 :

Un guide d'utilisation de la solution est mis à disposition des clients de l'organisme et mis à jour à chaque évolution.

Éléments d'auditabilité :

- Téléversement du guide d'utilisation de la solution correspondant à la version évaluée.

L'exigence 3.1 est imposée aux trois premières catégories.

Exigence 3.2 :

La solution permet d'assurer la traçabilité des actions exécutées, notamment à l'aide de tableaux de bord ou d'outils de suivi.

Éléments d'auditabilité :

- Téléversement d'un « printscreen » de l'interface permettant d'assurer la piste d'audit.
- Téléversement d'une extraction anonymisée d'un cas client.
- Téléversement d'un compte d'accès à une plateforme de démonstration pour que l'auditeur puisse vérifier

L'exigence 3.2 est imposée aux cinq catégories.

Exigence 3.3 :

L'organisme candidat assure une mise à disposition régulière des dernières versions des sources (non obfusquées) de la solution auprès d'un tiers de confiance qui pourra être sollicité en cas de besoin (par exemple pour assurer une continuité d'activité en cas de difficultés de l'éditeur).

Éléments d'auditabilité :

- Téléversement d'une preuve de dépôt liée à la dernière version actuellement en production auprès d'un tiers de confiance.

L'exigence 3.3 est imposée aux trois premières catégories.

Exigence 3.4 :

La solution sait déterminer s'il est nécessaire ou non d'effectuer une analyse d'impact relative à la protection des données et sait accompagner son exécution.

Éléments d'auditabilité :

- Téléversement du « printscreen » d'évaluation **des neuf critères** issus des lignes directrices du G29.
- Téléversement d'un PIA réalisé avec la solution.

L'exigence 3.4 est imposée à la seconde catégorie.

Exigence 3.5 :

La solution embarque un dispositif d'effacement paramétrable en production en fonction des durées de conservation des différents traitements qu'elle assure.

Éléments d'auditabilité :

- Téléversement du « printscreen » de l'interface dédiée.

L'exigence 3.5 est imposée aux cinq catégories.

Exigence 3.6 :

La solution assure le droit à la réversibilité de toutes les données traitées, ainsi que l'effacement des données à la suite d'un traitement de réversibilité.

Éléments d'auditabilité :

- Téléversement d'exemple d'export réutilisable de tous les traitements liés (xml, json, csv, xls).
- Téléversement d'un certificat d'engagement d'effacement type.

L'exigence 3.6 est imposée 3 premières catégories.

Exigence 3.7 :

La solution dispose d'une interface permettant d'assurer les différents droits des personnes, à destination du DPO pour la catégorie 2, à destination des personnes concernées pour les autres catégories.

Éléments d'auditabilité :

- Téléversement d'un « printscreen » de l'interface permettant d'assurer cette fonctionnalité pour la seconde catégorie.
- Mise à disposition d'un compte accès à une plateforme de démo pour la seconde catégorie.
- Mise à disposition d'un accès à l'espace dédié informant de la procédure à suivre pour toutes les catégories hormis la seconde.

L'exigence 3.7 est imposée aux cinq catégories.