PROCEDURE GENERALE DE CONFORMITE DONNEES PERSONNELLES

AXELERA

Mise à jour le 30 octobre 2025

Note interne – Diffusion générale

AXELERA est soucieuse de la protection de vos données personnelles et s'engage à assurer le meilleur niveau de protection et de sécurité de celles-ci en conformité avec la loi Informatique et Libertés n° 78-17 du 6 janvier 1978 modifiée (LIL) et au règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (règlement général pour la protection des données ou RGPD). (ci -après les « ***Dispositions relatives aux données personnelles*** »).

La protection des données personnelles et le respect de la vie privée sont une préoccupation de notre association.

La protection des données est l'œuvre de tous, il est donc important pour nous que vous soyez informés sur les mesures que nous avons mises en œuvre, celles que vous devez respecter et les droits que vous possédez.

Si vous avez la moindre question concernant cette règlementation, nous vous invitons à contacter notre Délégué à la Protection des Données.

Date	Rédigé par	Validé par :	Commentaires
3/11/2025	Fidal – Aurélie GARRET-DALMAIS		Version 1 de la politique général Données Personnel

Table des matières

1. IDENTITE DU DELEGUE A LA PROTECTION DES DONNEES 4
   1.1. Délégué à la protection des données ou Référent Données Personnelles : 4
      1.1.1. Désignation d'un DPD ? 4
      1.1.2. Justification de l'absence de désignation d'un DPD : 4
   1.2. Un délégué à la protection des données ça sert à quoi ? 4
   1.3. Indisponibilité ponctuelle du DPD ? 4
   1.4. Changement de DPD : Qui choisir ? 5
      1.4.1. Qui choisir ? 5
      1.4.2. Que faire ? 5
2. LA MISE EN PLACE D'UN TRAITEMENT DE DONNEES PERSONNELLES : 6
   2.1. Qu'est ce qu'une Donnée Personnelle et un traitement de données personnelles : 6
      2.1.1. Qu'est-ce qu'une « donnée personnelle » ? 6
      2.1.2. Qu'est-ce qu'une « donnée sensible » ? 6
      2.1.3. Qu'est-ce qu'un « traitement » de données ? 6
      2.1.4. Qu'est-ce qu'une modification /une création ? 6
   2.2. Quels sont les acteurs sur ce traitement de données : 7
      2.2.1. Qui est le Responsable de Traitement 7
      2.2.2. Qui est le Sous-Traitant 7
      2.2.3. Qui est le Co-traitant 7
   2.3. Quelles sont mes obligations en tant que Responsable de Traitement : 7
      2.3.1. Licéité du traitement : 7
      2.3.2. Information des personnes concernées : 9
      2.3.3. Efficience de l'exercice des droits : 11
      2.3.4. Sécurisation des transferts des données : 13
      2.3.5. Sécurisation des données : 14
      2.3.6. Documentation du traitement : 15
3. QUE FAIRE EN CAS DE VIOLATION DE DONNEES ET/OU DE CYBERATTAQUE ? 16
   3.1. Qu'est-ce qu'une cyberattaque ou une violation de données ? 16
   3.2. Isoler rapidement l'incident d'un point de vue technique ? 17
   3.3. Notification des violations de données auprès de la CNIL dans les 72heures 17
   3.4. Notification des personnes concernées 17
   3.5. Déclaration assurance 18
   3.6. Dépôt de plainte 18
4. LES CONTROLES DE LA CNIL : 18
5. ARRIVEE ET DEPART DES COLLABORATEURS – POINTS DE VIGILENCES : 19
   5.1. Procédure lors de l'arrivée d'un nouveau collaborateur 19

5.2. Formation continue des collaborateurs sur les dispositions relatives aux données personnelles 20
5.3. Changement de poste d'un collaborateur ou départ d'un collaborateur : 20
6. L'ARCHIVAGE DES DOCUMENTS ET LEUR MISE A JOUR 20

1. IDENTITE DU DELEGUE A LA PROTECTION DES DONNEES

Le responsable du traitement des données personnelles est :

L'ASSOCIATION AXELERA (Ci-après « AXELERA »)
Association régie par la loi du 1Er juillet 1901
SIRET : 485 210 082 00049,
Adresse : Les Levées- au rond -point de l'échangeur à Solaize (69360) – France
Déclaration de préfecture :

1.1. Délégué à la protection des données ou Référent Données Personnelles :

1.1.1. Désignation d'un DPD ?

AXELERA a fait le choix de désigner un Délégué à la Protection des données.

Le Délégué à la Protection des Données (DPD) au sein de l'association AXELERA est :

Nom	Frédéric Laroche
Adresse	Les levées – Au rond-point de l'échangeur à Solaize (69360)
Email	Rgpd.axelera@axelera.org
Téléphone	06 68 66 98 06

Le DPD a été désigné officiellement auprès de la CNIL le 9 octobre 2024 – (Désignation n°DPO -15 770).

Pour toute modification des coordonnées et/ou informations relative au DPD : https://www.cnil.fr/fr/designation-dpo

1.1.2. Justification de l'absence de désignation d'un DPD :

N/A

1.2. Un délégué à la protection des données ça sert à quoi ?

Le délégué à la protection des données (DPD) veille au respect du Règlement Général sur la Protection des Données (RGPD) et de la Loi Informatique et Libertés (LIL) au sein d'une organisation.

Il conseille, contrôle et alerte sur les pratiques de traitement des données personnelles.

Il sert de point de contact entre l'organisme, les personnes concernées et l'autorité de contrôle comme la CNIL.

ATTENTION, il doit être joignable au numéro et adresse email indiqué dans le formulaire de désignation rapidement. Certaines actions doivent être effectuées sous 72 heures.

1.3. Indisponibilité ponctuelle du DPD ?

En cas d'absences ponctuelles du DPD, qu'elles soient dues à une carence, une maladie ou des vacances, il est nécessaire de :

- **Identifier les risques liés à l'absence** : il s'agira de cartographier les missions critiques du DPD (suivi des traitements, réponses aux demandes de droits, audits, etc.). Le DPD devra pour cela tenir un carnet de bord à jour de ses missions en cours/ urgentes/ non urgentes
- **Désigner un DPD suppléant, le former et l'informer:** il sera nécessaire de nommer un DPD adjoint ou un référent RGPD formé aux enjeux de la protection des données en attendant le retour du DPD

- **Mettre en place un message d'absence sur la boite email du DPD avec renvoi vers le DPD suppléent**
- **Communication interne** : Informer les équipes de la personne référente pendant l'absence du DPD
- **Maintenir une documentation claire et accessible pour faciliter la prise de relais**
- **Organiser un point de passation au retour du DPD**

1.4. Changement de DPD : Qui choisir ?

1.4.1. Qui choisir ?

Le choix du DPD doit se porter sur une personne possédant une expertise solide en matière de droit et de pratiques en protection des données personnelles. Elle doit comprendre les enjeux du RGPD, maîtriser les processus de traitement de données au sein de l'entreprise, et être capable de dialoguer avec les autorités de contrôle comme la CNIL. Ce rôle exige également une indépendance dans l'exercice de ses missions, une capacité à sensibiliser les équipes, et à conseiller la direction sur les risques liés aux données.

Il peut s'agir :

- d'un salarié interne, à condition qu'il ait les compétences requises et qu'il soit placé dans une position qui garantit son autonomie.
- d'un prestataire externe dédié
- d'un prestataire externe mutualisé

Dans tous les cas, **le DPD doit avoir accès aux ressources nécessaires** pour accomplir ses missions efficacement et être clairement identifié dans l'organigramme et les communications officielles.

Le DPD ne doit pas se trouver en situation de conflit d'intérêts, c'est-à-dire qu'il ne peut exercer des fonctions qui l'amèneraient à déterminer les finalités ou les moyens des traitements de données personnelles.

1.4.2. Que faire ?

Lorsqu'une entreprise change de Délégué à la Protection des Données (DPD), elle doit :

- **Immédiatement informer la CNIL**, en ligne, **de la fin de mission de l'ancien DPD** : Connexion | CNIL Pro Professionnel
- **Choisir le nouveau DPD**, en interne ou en externe
- En interne, faire signer au DPD désigné **la fiche de mission DPD / en externe faire s**igner un contrat de Prestation de DPO externalisé. Attention, le document doit être revu avant signature par la direction et le service juridique.
- **Effectuer une nouvelle désignation de DPO : .** La CNIL détaille le processus sur le lien suivant : Désigner un délégué à la protection des données (DPO) ou modifier une désignation | CNIL
- **Mettre à jour le registre des traitements** pour **modifier** les coordonnées du nouveau DPD.
- **Mettre à jour les registres des droits** pour **modifier** les coordonnées du nouveau DPD.
- **Mettre à jour le registre des violations** pour **modifier** les coordonnées du nouveau DPD.
- **Modifier la (es) politique(s) de confidentialité** pour **modifier** les coordonnées du nouveau DPD.
- **Mettre à jour la procédure de durée** pour **modifier** les coordonnées du nouveau DPD.

- **Mettre à jour la procédure générale Données Personnelles** pour **modifier** les coordonnées du nouveau DPD.
- **Mettre à jour les analyse d'impact** pour **modifier** les coordonnées du nouveau DPD.
- **Mettre à jour l'ensemble des modèles types de contrat où figurent des coordonnées du DPD**
- **Actualiser les autres supports de communication**
- **Informer les équipes internes** : Il s'agit de communiquer officiellement le changement de DPD à tous les collaborateurs, notamment ceux impliqués dans le traitement des données (RH, marketing, IT…). Cela renforce la transparence et facilite les échanges futurs.
- **Prévoir, si possible, une période de passation entre l'ancien DPD et le nouveau DPD** pour assurer la continuité des missions, notamment sur les audits en cours ou les recommandations en attente.
- **Documenter la transition** afin de conserver une trace écrite des étapes du changement.

2. LA MISE EN PLACE D'UN TRAITEMENT DE DONNEES PERSONNELLES :

2.1. Qu'est ce qu'une Donnée Personnelle et un traitement de données personnelles :

2.1.1. Qu'est-ce qu'une « donnée personnelle » ?

Une donnée personnelle est une information se rapportant à une personne physique directement ou indirectement. Par exemple, peuvent être considérées comme des données personnelles, un identifiant, un nom, un numéro d'identification, une adresse IP, une photographie, un numéro de téléphone (…).

2.1.2. Qu'est-ce qu'une « donnée sensible » ?

Parmi les données personnelles, figurent les données sensibles. Il s'agit notamment de l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes, sauf si leur traitement est rendu nécessaire par une disposition législative ou une mission d'intérêt publique

2.1.3. Qu'est-ce qu'un « traitement » de données ?

Un traitement de données personnelles se définit comme toute opération sur les données à caractère personnel : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. En synthèse toute opération utilisant et/ou consultant vos données.

2.1.4. Qu'est-ce qu'une modification /une création ?

Un **nouveau traitement** désigne toute opération ou ensemble d'opérations portant sur des données personnelles qui n'était pas encore mis en œuvre dans l'organisation. Cela peut être, par exemple, la mise en place d'un nouvel outil de gestion des candidatures, d'un système de suivi des appels clients, ou encore d'une application interne de gestion des temps.

La **modification d'un traitement** existant intervient lorsqu'un traitement déjà en place évolue de manière significative. Cela peut concerner l'ajout de nouvelles finalités, l'intégration de nouvelles catégories de données, un changement dans les destinataires ou les modalités de conservation.

Quoi	Qui
1 - Identifier si on est en présence d'une Donnée Personnelle, s'il s'agit d'une donnée sensible et si on est dans le cadre d'un traitement.	Tout collaborateur
2- Informer immédiatement le DPD de l'existence d'un traitement de données personnelles	Tout collaborateur

2.2. Quels sont les acteurs sur ce traitement de données :

2.2.1. Qui est le Responsable de Traitement

Le **Responsable du Traitement** est la personne qui, seule ou conjointement avec d'autres, **détermine les finalités et les moyens d'un traitement de données** (Le Pourquoi et le Comment).

2.2.2. Qui est le Sous-Traitant

Le sous-traitant est celui qui traite des données à caractère personnel pour le compte du Responsable du Traitement.

2.2.3. Qui est le Co-traitant

Il peut arriver qu'un responsable de traitement ne soit pas le seul organisme à définir les finalités et les moyens du traitement, il peut le faire conjointement avec un autre organisme. On parle alors de co-traitance

Quoi	Qui
3 - Identifier pour chaque traitement qui est le Responsable, s'il est seul responsable ou co-responsable ou s'il agit en sous-traitance ou s'il fait appel à des sous-traitants	DPD – Assistant à DPO

2.3. Quelles sont mes obligations en tant que Responsable de Traitement :

Pour chaque traitement de données personnelles, pour lequel AXELERA est Responsable de traitement, il est nécessaire de :

1. S'assurer de la licéité du traitement des données d'AXELERA (étape 1)
2. Vérifier si les personnes concernées par le traitement de leurs données ont été informées (étape 2).
3. Vérifier si AXELERA respecte les droits des personnes concernées (étape 3).
4. S'assurer que AXELERA maîtrise le transfert de ses données (étape 4).
5. S'assurer que les données collectées soient sécurisées (étape 5).
6. S'assurer que AXELERA a documenté le respect de ses obligations. (étape 6).

2.3.1. Licéité du traitement :

Pour qu'un traitement soit licite, il doit respecter les principes suivants :

2.3.1.1. Principe de loyauté et transparence = Base légale

Les principes de loyauté et de transparence imposent que le Traitement de données à caractère personnel de l'intéressé ne doit pas être fait à son insu et doit soit avoir reçu **le consentemen**t de la personne concernée soit satisfaire à l'une des conditions suivantes (ci-après la « Base juridique du traitement ») :

- Le **respect d'une obligation légale** incombant au responsable du traitement ;
- La **sauvegarde de la vie** de la personne concernée ;
- L'**exécution d'une mission de service public** dont est investi le responsable ou le destinataire du traitement ;
- L'**exécution, soit d'un contrat** auquel la personne concernée est partie, soit des mesures précontractuelles prises à la demande de celle-ci ;
- La réalisation de l'**intérêt légitime** poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Si le recueil du consentement est érigé au rang de principe, la nature des exceptions permet en pratique de se dispenser d'une telle exigence dans différentes circonstances

Quoi	Qui
4 - Identifier pour chaque traitement la base légale applicable	DPD – Assistant à DPO

2.3.1.2. Principe de limitation des finalités

Les Données doivent être collectées **pour des finalités déterminées** (ex : effectuer des opérations relatives à la gestion des adhérents concernant les contrats et les commandes), explicites et légitimes et ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités.

Quoi	Qui
5 - Identifier pour chaque donnée quelles sont les finalités	DPD – Assistant à DPO

2.3.1.3. Principe de minimisation des données

Les Données collectées et/ou traitées doivent être adéquates, pertinentes et limitées à ce qui est strictement nécessaire au regard des finalités pour lesquelles elles ont été collectées et de leurs traitements ultérieurs.

En d'autres termes, seules les données nécessaires et compatibles avec la finalité envisagée peuvent être légitimement collectées.

Cas particuliers des zones de commentaires libres : Les zones de commentaires libres dans les outils professionnels peuvent sembler anodines, mais elles représentent un véritable enjeu en matière de protection des données personnelles. **Pour respecter les dispositions sur les données personnelles, il est essentiel que tous les collaborateurs adoptent une approche rigoureuse et responsable lorsqu'ils les remplissent**. Il est primordial de respecter les règles suivantes :

- Eviter au maximum ; les zones de commentaires libres
- Chaque fois, qu'il y a des zones de commentaires libres, indiquer aux collaborateurs le warning ci-dessous :
    - Les informations saisies doivent rester strictement factuelles et pertinentes par rapport à l'objectif du traitement. Il est impératif d'éviter tout jugement de valeur, propos subjectif ou formulation émotionnelle. Par exemple, au lieu d'écrire qu'un client est "désagréable", il convient de noter qu'il "a exprimé son mécontentement concernant le service reçu".
    - Il est interdit de mentionner des données dites « sensibles », comme l'état de santé, les opinions politiques, les croyances religieuses ou l'origine ethnique. Ces informations sont encadrées de manière stricte par le RGPD et ne doivent jamais apparaître dans une zone de commentaire libre, sauf dans des cas très spécifiques et le cas échéant, avec le consentement explicite de la personne concernée.

Il faut garder à l'esprit que toute personne a le droit d'accéder aux données qui la concernent. Cela signifie que les commentaires saisis peuvent être lus par les individus visés. Il est donc essentiel d'écrire avec professionnalisme, comme si le message allait être partagé directement avec la personne.

Quoi	Qui
6 - Identifier pour chaque traitement, les données qui ne sont pas utiles et les supprimer	DPD – Assistant à DPO

2.3.1.4. Principe d'exactitude

Les Données doivent être exactes, complètes et si nécessaire mises à jour. Cette obligation implique de mettre en place des mesures adaptées pour permettre la rectification ou la mise à jour des informations collectées ainsi que leur suppression lorsqu'elles deviennent obsolètes.

Quoi	**Qui**
7 – Mettre en place pour chaque traitement, avec le responsable interne concerné, le cycle de vie de la donnée	DPD – Assistant à DPO Responsable interne en charge du traitement
8 – Corriger les données dans les différents canaux et/ou supprimer celles obsolètes	DPD – Assistant à DPO Responsable interne en charge du traitement

2.3.1.5. Durée limitée

Le RGPD impose le principe de limitation de la conservation : les données personnelles ne doivent être conservées que pendant une durée strictement nécessaire à la finalité du traitement. Cette durée doit être définie dès la conception du traitement, en tenant compte des obligations légales (ex. : 10 ans pour les factures), des besoins opérationnels, et du principe de minimisation.

Ainsi, il appartient au responsable de traitement de gérer la durée de conservation de données de manière conforme à cette exigence et de mettre en place une procédure de purge des données.

Il est possible de se baser :

- sur la délibération CNIL n°2005-213 du 11 octobre 2005 relative à l'archivage des données Délibération 2005-213 du 11 octobre 2005 - Légifrance
- le guide des durées de conservation de la CNIL (version 2020) Guide pratique : Les durées de conservation
- Sur la politique **interne d'archivage - +++++**

Quoi	**Qui**
9 – Définir une durée de conservation des données	DPD – Assistant à DPO Responsable interne en charge du traitement
10 – S'assurer que techniquement ladite donnée puisse être supprimée et/ou modifiée à cette échéance	DPD – Assistant à DPO Responsable interne en charge du traitement
11- Si ajout d'un nouveau délai, intégrer ce nouveau délai dans la procédure d'archivage et purge des données	DPD – Assistant à DPO

2.3.2. Information des personnes concernées :

Il appartient au responsable de traitement d'informer les personnes concernées d'une part sur la collecte de leurs données (qui a collecté quand, comment et pourquoi) et de leurs droits et en particulier, le responsable doit fournir les informations suivantes :

- L'identité et les coordonnées du responsable de traitement, et, du représentant du responsable du traitement (pour les établissements situés dans un pays autre que le lieu où est situé le responsable)
- Les coordonnées du délégué à la protection des données (également appelé « DPD » ou « DPO »), s'il y a lieu

- La finalité poursuivie par le traitement et la base juridique du traitement (notamment si fondé sur l'existence d'un intérêt légitime, définir cet intérêt légitime),
- Les destinataires ou catégories de destinataires des données,
- Le cas échéant, des transferts de données envisagés à destination d'un Etat non-membre de l'Union Européenne ou à une organisation internationale,
- La durée de conservation des données ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée,
- les droits dont elles disposent concernant ces données, à savoir : un droit d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition au traitement, et d'un droit à la portabilité des données, d'un droit de retrait du consentement à tout moment (lorsque la collecte des données est fondée sur le consentement), ainsi que du droit de définir des directives générales et particulières définissant la manière dont la personne concernée entend que soient exercés, après son décès, ces droits. Chaque personne concernée par la collecte de ses données personnelles dispose également du droit d'introduire une réclamation auprès d'une autorité de contrôle (à savoir, en France, la CNIL).
- Si la collecte repose sur une obligation légale ou contractuelle et les conséquences d'un éventuel refus de fournir les données
- L'existence d'une prise de décision automatisée, y compris d'un profilage. Le profilage étant défini comme toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique
- Si le responsable a l'intention d'effectuer un traitement ultérieur des Données pour une finalité différente.

Dans l'hypothèse où les données n'auront pas été recueillies directement auprès de la personne concernée (**collecte indirecte**), le responsable du traitement ou son représentant doit alors fournir à cette personne, outre les différentes informations précitées, **la source d'où proviennent les données** avec la mention indiquant qu'elles sont issues d'une source accessible au public ou non ainsi que **les catégories de données à caractère personnel concernées**.

Cette information s'effectue de manière claire et précise, à la fois :

- Sur les formulaires de collectes
- Dans les politiques données personnelles mises en place

A date, AXELERA dispose des Politique Données Personnelles suivantes :

- Politique DCP Adhérents – Prospects – Clients Axelera
- Politique DCP collaborateurs AXELERA
- Politique DCP fournisseurs AXELERA

Commenté [AG1]: Mettre un lien vers lesdites Politiques Données Personnelles

Une mention type sur les formulaires de collecte doit également être adaptée et insérée :

« Les informations recueillies ++++++ [Indiquer le support de la collecte] sont destinées à +++++ [Indiquer la finalité principale]. Elles font l'objet d'un traitement destiné à l'association AXELERA et sont notamment collectées sur la base de +++++[Indiquer la ou les bases légales]. Les informations identifiées par un astérisque sont obligatoires. A défaut, votre demande ne pourra pas être traitée ou son traitement sera retardé. Vous disposez d'un droit d'accès d'interrogation, de modification et de rectification aux informations qui vous concernent. Vous disposez également d'un droit d'opposition au traitement de vos données à caractère personnel pour des motifs légitimes, ainsi que d'un droit d'opposition à ce que ces données soient utilisées

à des fins de prospection commerciale. Vous disposez enfin du droit de définir des directives générales et particulières définissant la manière dont vous entendez que soient exercés, après votre décès, ces droits.

Pour exercer vos droits, vous devez adresser un courriel à l'adresse suivante, à l'attention de notre délégué à la protection des données :rgpd.axelera@axelera.org

Nous vous invitons également à consulter notre Politique de confidentialité des données +++[Indiquer la politique DCP concernée] accessible ++++[indiquer où se trouve cette Politique DCP] pour avoir plus d'informations sur le traitement de vos données (destinataires, base(s) légale(s), durée de conservation…)et à nous contacter pour toute autre question complémentaire. »

Quoi	Qui
12 – Ajouter le traitement dans le politique DCP concernée et Informez les personnes concernées de la modification de la politiques DCP	DPD – Assistant à DPO
13 – Ajouter une mention sur le formulaire de collecte	DPD – Assistant à DPO

2.3.3. Efficience de l'exercice des droits :

Les personnes concernées par le traitement de leurs données doivent être non seulement informées de leurs droits, mais la mise en œuvre de ces droits doit être effective. En l'occurrence et si un adhérent, fournisseur, prestataire, partenaire ou un salarié sollicite un droit d'accès s'agissant des données le concernant, il est nécessaire d'y répondre en respectant un délai imposé par le RGPD.

Lorsqu'une personne concernée souhaite exercer ses droits, elle peut le faire par tout moyen : courrier, e-mail, formulaire en ligne, ou même verbalement.

Les droits des personnes concernées sont :

Droits	Description	Les limites à ce droit
Droit à l'information	Être informé de manière claire sur la collecte et l'usage des données personnelles.	N/A
Droit d'accès	Obtenir une copie des données personnelles détenues par un organisme.	- Demandes manifestement abusives - Atteinte aux droits des tiers
Droit de rectification	Corriger des données inexactes ou incomplètes.	N/A
Droit à l'effacement (ou « droit à l'oubli »)	Demander la suppression des données dans certains cas.	- Respect d'une obligation légale - Mission d'intérêt public
Droit à la limitation du traitement	Restreindre temporairement l'usage des données.	N/A
Droit à la portabilité	Récupérer ses données dans un format structuré et les transmettre à un autre responsable.	- Respect d'une obligation légale - Mission d'intérêt public - Intérêt légitime
Droit d'opposition	S'opposer à certains traitements, notamment à des fins de prospection.	- Respect des libertés et droits fondamentaux - Respect d'une obligation légale
Droit de ne pas faire l'objet d'une décision automatisée	Refuser qu'une décision soit prise uniquement par un algorithme	N/A

Droit de définir des directives sur le sort de ses données après sa mort	Statuer si on souhaite l'effacement, la continuation du traitement après sa mort	N/A

L'exercice de ces droits doit être effectif, **dans un délai d'un mois**.

La CNIL indique dans ses recommandations sur le sujet que le principe demeure: « *pas de pièce d'identité, sauf en cas de doute raisonnable* ». (Répondre aux demandes d'exercice des droits | CNIL)

Il convient de se référer aux lignes directrices de la CEPD sur les droits d'accès edpb_guidelines_202201_data_subject_rights_access_v2_fr.pdf.

Il convient de conserver la trace des éléments de réponses, à la suite d'une demande, et donc de remplir le tableau Registre des Droits des Personnes.

En cas de demande complexe liée aux droits des personnes, notamment sur la portabilité, droit d'accès ou effacement des données, il est fortement recommandé de faire appel à un avocat. Ces demandes peuvent soulever des enjeux techniques et juridiques sensibles : quelles données sont concernées, dans quel format les transmettre, à qui, et dans quelles conditions. Une mauvaise interprétation ou une réponse incomplète peut entraîner des risques juridiques importants, notamment en cas de plainte ou de contrôle par la CNIL.

Quoi	**Qui**
14 – Informer immédiatement le DPD, en cas de demande de droit des personnes concernée	Tout collaborateur d'AXELERA
15 – Analyse des suites à donner : - **Est-ce que la demande est conforme aux modalités de saisine** - **Est-ce que l'auteur de la demande est une personne concernée** - **Est-ce qu'il existe une limite aux droits** - **Est-ce que des tiers sont concernées par cette demande**	DPD – Assistant à DPO
16 – Informer dans le mois de la saisine la personne concernée des suites à donner : - **Refus doit être motivé (ex : fondement obligation légale)** - **Demande d'information complémentaire (par exemple communication d'une pièce d'identité pour s'assurer de l'auteur de la demande)** - **Demande d'un délai complémentaire de deux (2) mois, en motivant les raisons d'un tel délai (ex : la complexité et du nombre de demandes), à condition que la personne concernée ait été informée des raisons de ce retard dans un délai d'un mois à compter de la réception de la demande**	DPD – Assistant à DPO
17- Communiquer à la personne concernée les éléments demandés : - **Communiquer TOUTES les données, mais QUE les données (donc caviarder tous les éléments relatifs à des tiers, y compris autres salariés)** - **Mode de communication : une copie ou un accès sur place**	DPD – Assistant à DPO Avec l'aide du responsable du ou des services concernés
18- Remplir le Registre Exercice des Droits des Personnes concernées	DPD – Assistant à DPO

2.3.4. Sécurisation des transferts des données :

Choisir un prestataire qui respecte le RGPD est une exigence fondamentale pour toute organisation qui traite des données personnelles. En effet, dès qu'un prestataire intervient dans le cadre d'un traitement, que ce soit pour héberger des données, fournir un logiciel, gérer des campagnes marketing ou assurer un service client. Travailler avec un prestataire non conforme expose AXELERA à des **risques juridiques et financiers importants**. En cas de manquement, la responsabilité du responsable de traitement (c'est-à-dire l'entreprise qui fait appel au prestataire) peut être engagée.

La réglementation Informatique et Libertés et le RGPD encadrent le transfert de données à caractère personnel **à des tierces personnes**, notamment situées à l'étranger, c'est-à-dire hors de l'Union Européenne. La réglementation Informatique et Libertés et le RGPD prévoient que le transfert de données à caractère personnel vers des pays hors Union Européenne (donc y compris UK et la Suisse…) ou des organisations internationales n'est possible que si :

- Le transfert est fondé sur une décision de la Commission européenne (= Décision d'adéquation) explicitant que le pays tiers ou l'organisation internationale en question assure un niveau de protection adéquat, ou,
- Le responsable de traitement ou le sous-traitant a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives telles que :
  - clauses types de transferts des données hors Union Européenne,
  - Règles d'entreprise contraignantes),
- A défaut, obtenir l'autorisation préalable de la CNIL ou de la Commission Européenne.

De plus, y compris lorsque les transferts ont lieu au sein de l'UE, les contrats avec les sous-traitants et/ou les co-responsables doivent être écrits et prévoir des clauses garantissant le respect de la règlementation sur les données personnelles.

Les modèles de contrat de sous-traitance et de co-traitance sont mis à dispositions, et devront être complétés et validés avant envoi au partenaire concerné.

En cas de doute sur la qualification d'un prestataire, responsable du traitement, sous-traitant ou co-responsable, il est vivement recommandé de consulter un avocat. Une mauvaise qualification peut entraîner des conséquences juridiques sérieuses : responsabilité engagée en cas de violation, non-respect des obligations contractuelles, ou encore sanctions de la CNIL. Le RGPD impose une rigueur absolue dans la répartition des rôles, et une erreur d'analyse peut compromettre la conformité globale du traitement.

Quoi	**Qui**
19 – Communiquer pour tout nouveau prestataire sélectionné, le projet de contrat au DPD	Tout collaborateur d'AXELERA
20 – Analyse les flux de données avec les tiers, afin de déterminer, si le prestataire intervient : - **En qualité de Responsable de Traitement Autonome** - **En qualité de Sous-traitant** - **En qualité de co-responsable de traitement**	DPD – Assistant à DPO
21 –En fonction de l'analyse réalisée, et en l'absence de clause RGPD conforme dans le contrat du prestataire, adresser l'un des contrats requis au prestataire et assurer le suivi de sa signature	DPD – Assistant à DPO

22 – En cas de transfert des données Hors UE, vers un pays ne disposant pas d'une décision d'adéquation, rédiger des clauses contractuelles types	DPD – Assistant à DPO
23- Compléter le Tableau des Prestataires	DPD – Assistant à DPO

2.3.5. Sécurisation des données :

Les Dispositions relatives aux Données Personnelles **précisent que la protection des données personnelles nécessite de prendre des « *mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».** Cette sécurité doit passer par une sécurité logique et physique, notamment l'accès des bâtiments dans lesquels les données sont conservées doit être spécialement contrôlé et la liste des personnes pouvant accéder à ces données doit être strictement établie. Le RGPD conseille l'adoption d'un code de conduite, et ou de mécanisme de certification pour démontrer le respect de ces exigences.

La CNIL a édité plusieurs guides relatifs à la sécurité des traitements présentant un ensemble de préconisations : Guide de la sécurité des données personnelles | CNIL. Il convient de vérifier que ces règles minimales sont respectées.

L'article 4.12) du RGPD définit une violation de données à caractère personnel comme

> *« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.*

Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

Exemples :

- suppression accidentelle de données conservées par AXELERA et non sauvegardées par ailleurs;
- perte d'une clef USB non sécurisée contenant une copie de la base de données des adhérents ;
- introduction malveillante dans une base de données CRM

Le responsable de traitement, a l'obligation de notifier :

- Dans tous les cas, compléter le Registre des Violations
- D'une part, à la CNIL toute violation des données à caractère personnel susceptible d'engendrer **un risque** pour les droits et libertés des personnes physiques dans les 72 heures au plus tard après en avoir pris connaissance : https://notifications.cnil.fr/notifications/index
- D'autre part, de communiquer aux personnes concernées l'existence d'une telle violation **en cas de risque élevé.**

Cette même obligation pèse sur le sous-traitant.

Quoi	**Qui**
24 – Effectuer une revue régulière des règles de sécurité physique et logique	Tout collaborateur d'AXELERA
25 – S'assurer de la signature de NDA pour l'ensemble des collaborateurs et prestataires externes	DPD – Assistant à DPO
26 –Mettre à jour régulièrement les règles d'habilitation, et à chaque entrée et départ de tout collaborateur	DPD – Assistant à DPO

27 – En cas de violation de données personnelles, informer le DPO	DPD – Assistant à DPO
28 – Analyse le risque pour les personnes concernées : - **Aucun risque** - **Un risque** - **Un risque Elevé**	DPD – Assistant à DPO
29 – Si aucun risque : documenter le Registre des Violations	DPD – Assistant à DPO
30 – Si existence d'un risque : - **Documenter le Registre des Violations** - **Notifier à la CNIL sous 72 heures (possibilité de faire une notification préalable puis notification plus complète)** - **Informer les sous-traitants et autres responsables de traitements** - **Prévenir assurance** - **Eventuellement, effectuer un dépôt de plainte**	DPD – Assistant à DPO
31 – Si existence d'un risque : - **Documenter le Registre des Violations** - **Informer les sous-traitants et autres responsables de traitements** - **Notifier à la CNIL sous 72 heures** - **Informer les personnes concernées, sauf si existence de mesures techniques préventives suffisantes, ou si mesures curatives suffisantes ou si communication exigerait des efforts disproportionnés** - **Prévenir assurance** - **Eventuellement, effectuer un dépôt de plainte**	DPD – Assistant à DPO

2.3.6. Documentation du traitement :

Le RGPD repose sur **le principe d'accountability** : chaque organisme doit être capable de démontrer sa conformité à tout moment. Cela passe par une documentation rigoureuse et actualisée, qui constitue la preuve de la mise en œuvre des obligations légales.

Cela inclut :

- la tenue d'un registre des traitements,
- la réalisation d'analyses d'impact pour les traitements à risque,
- la mise en place de déclaration et/ou demande d'autorisation auprès de la CNIL : Non concernée pour AXELERA

Cette documentation n'est pas seulement une exigence réglementaire, elle constitue une véritable stratégie de transparence et de maîtrise des risques. Elle permet à l'organisation de démontrer sa responsabilité, de faciliter les audits, et de réagir efficacement en cas de contrôle ou d'incident. En résumé, c'est le socle opérationnel de la conformité RGPD, à la fois juridique, technique et organisationnel.

2.3.6.1. La tenue d'un registre des traitements

L'article 30 du RGPD prévoit la tenue d'un registre du responsable de traitement de données personnelles et d'un registre du sous-traitant.

L'obligation de tenir un registre des traitements concerne tous les organismes, publics comme privés et quelle que soit leur taille, dès lors qu'ils traitent des données personnelles.

Le registre des traitements doit être tenu à jour par le DPO.

Attention, si vous intervenez en tant que sous-traitant, vous devrez disposer d'un registre des traitements sous-traités. A date, AXELERA n'intervient pas en tant que sous-traitant.

Quoi	Qui
32 – Pour chaque nouveau traitement transmis, le DPO doit l'intégrer dans le Registre des traitements, en prenant soin de modifier la date du document	DPD – Assistant à DPO

2.3.6.2. La mise en place d'analyse d'impact

Si le traitement est susceptible d'engendrer un risque élevé (par exemple, en cas de surveillance systématique ou de profilage) une analyse d'impact sur la protection des données (AIPD) doit être réalisée. Cette analyse permet d'identifier les mesures techniques et organisationnelles à mettre en place pour limiter les risques.

Le RGPD prévoit trois cas dans lesquels le PIA est obligatoire :

- Evaluation systématique et approfondie d'aspects personnels
- Traitement à grande échelle de catégorie particulières de données (ex : données de santé et/ou condamnation pénale)
- Surveillance systématique à grande échelle de zone accessible au public

L'autorité de contrôle (la CNIL) va par ailleurs régulièrement mettre à jour une liste des types d'opération de traitement pour lesquels un PIA sera obligatoire (Cf. Recommandation n°2018-327 du 11 octobre 2018).

La CNIL a également élaboré une liste de traitements pour lesquels elle n'estime pas nécessaire qu'une AIPD soit réalisée.

Pour savoir si un nouveau traitement nécessite ou non, une analyse d'impact, il convient de suivre le Guide la CNIL : L'analyse d'impact relative à la protection des données (AIPD) | CNIL

A date, AXELERA ne met pas en œuvre de traitements nécessitant une analyse d'impact.

Quoi	Qui
33 – Pour chaque nouveau traitement transmis, le DPO doit analyse si une analyse d'impact est requise	DPD – Assistant à DPO
34 – Dans l'affirmative, effectuer l'analyse d'impact	DPD – Assistant à DPO
35 – Pour chaque analyse d'impact effectuée, réaliser un suivi au moins annuel, pour s'assurer que le plan d'action est respecté	DPD – Assistant à DPO

3. QUE FAIRE EN CAS DE VIOLATION DE DONNEES ET/OU DE CYBERATTAQUE ?

3.1. Qu'est-ce qu'une cyberattaque ou une violation de données ?

Une cyberattaque est une action malveillante menée par un individu ou un groupe visant à compromettre la sécurité d'un système informatique. Elle peut prendre la forme d'un vol de données, d'un rançongiciel (ransomware), d'une intrusion dans les serveurs, ou d'une paralysie des systèmes

Une violation de données personnelles désigne tout incident de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données

personnelles. Cela peut résulter d'un piratage, d'une erreur humaine, d'un vol de matériel ou d'un mauvais paramétrage d'un outil informatique.

Quoi	Qui
36 – Informer immédiatement le DPD et le DSI	Tout collaborateur

3.2. Isoler rapidement l'incident d'un point de vue technique ?

Dès la détection ou la suspicion d'une violation de données personnelles ou de cyberattaque, il est impératif d'alerter immédiatement la Direction des Systèmes d'Information (DSI) ou le prestataire informatique en charge de la sécurité.

Ce sont eux qui disposent des compétences techniques pour 1) identifier la source et 2) isoler les systèmes compromis, 3) identifier l'ampleur de l'incident, 4) mettre en place les mesures correctives techniques et 5) conserver les preuves des différents points d'étapes ;

Quoi	Qui
37 – Informer immédiatement le DSI	Tout collaborateur/DPD
38 - Identifier la source et 2) isoler les systèmes compromis, 3) identifier l'ampleur de l'incident , 4) mettre en place les mesures correctives techniques	Le DSI
39 – Conserver la preuve de ces différents éléments en remplissant le Registre des Violations	DPD – Assistant à DPO Avec l'aide du DSI

3.3. Notification des violations de données auprès de la CNIL dans les 72heures

Si la violation présente un risque pour les droits et libertés des personnes, elle doit être notifiée à la CNIL dans un délai de 72 heures après en avoir eu connaissance. Cette notification se fait via le service en ligne de la CNIL. Elle doit contenir une description de l'incident, les données concernées, les conséquences possibles et les mesures prises.

Lien suivant pour réaliser la notification : Notifier une violation de données personnelles | CNIL

Quoi	Qui
40 – Si l'incident présente un risque, notifier à la CNIL dans les 72 heures	DPD – Assistant à DPO Avec l'aide du DSI

3.4. Notification des personnes concernées

Si la violation présente **un risque élevé** pour les personnes (ex. : usurpation d'identité, atteinte à la vie privée), celles-ci doivent être informées dans les meilleurs délais. L'information doit être claire, accessible et permettre aux personnes de prendre les mesures nécessaires pour se protéger.

Attention la notification aux personnes concernées n'est pas automatique. Nous vous invitons à prendre attache auprès d'un avocat afin qu'il vous accompagne sur ces démarches (vérification d'une présence d'une violation de données, réalisation de la notification auprès de la CNIL, nécessité ou non de notifier la violation auprès des personnes concernées…).

Quoi	Qui
41 – Si l'incident présente un risque élevé, informer les personnes, avec le concours éventuel d'une agence de communication et service juridique	DPD – Assistant à DPO Avec l'aide du service juridique et d'une agence de communication

3.5. Déclaration assurance

Si AXELERA dispose d'une assurance cybersécurité ou responsabilité civile, il est recommandé de déclarer l'incident rapidement.

Quoi	Qui
42 – Effectuer une déclaration auprès de votre assureur	DPD – Assistant à DPO Direction

3.6. Dépôt de plainte

En cas d'acte malveillant avéré (intrusion, vol, piratage), un dépôt de plainte auprès des autorités compétentes (police, gendarmerie) peut être nécessaire.

Cela permet de documenter l'incident, d'ouvrir une enquête, et de renforcer la légitimité des démarches entreprises.

Quoi	Qui
43 –Effectuer un dépôt de plainte	DPD – Assistant à DPO Direction

4. LES CONTROLES DE LA CNIL :

La CNIL peut intervenir selon plusieurs modalités, toutes encadrées par sa charte des contrôles : Contrôles de la CNIL : une charte pour tout comprendre | CNIL

- **Contrôle sur place** : les agents se rendent physiquement dans les locaux de l'organisme pour examiner les dispositifs de traitement et de sécurité.
- **Contrôle sur pièces** : l'organisme est invité à transmettre des documents (registre des traitements, AIPD, politiques de confidentialité, etc.).
- **Contrôle en ligne** : la CNIL analyse les éléments accessibles publiquement sur les sites web (cookies, formulaires, mentions légales…).
- **Audition** : les responsables peuvent être convoqués dans les locaux de la CNIL pour répondre à des questions précises.

Ces contrôles peuvent être déclenchés à la suite d'une plainte, d'un signalement, ou de manière proactive dans le cadre du programme annuel de vérification.

En cas de contrôle, il est essentiel d'adopter une posture transparente, coopérative et structurée.

- Prévenir immédiatement le DPD, qui coordonnera la réponse et les échanges avec la CNIL.
- Rassembler les documents clés : registre des traitements, analyses d'impact, politiques internes, contrats avec les sous-traitants, preuves de consentement, etc.

- Faciliter l'accès aux informations demandées, sans dissimulation ni obstruction. La CNIL peut demander des accès aux systèmes, des copies de fichiers ou des entretiens.
- Documenter les échanges et conserver une trace de toutes les communications et actions entreprises
- Rester factuel et professionnel dans les réponses.

En cas de contrôle de la CNIL, faire appel à un avocat est vivement recommandé. Ce type de contrôle peut avoir des implications juridiques sérieuses, notamment en cas de non-conformité ou de mauvaise interprétation des obligations du RGPD. L'avocat joue un rôle clé pour sécuriser les échanges, préparer les documents requis, encadrer les réponses et anticiper les suites éventuelles. Son expertise permet de limiter les risques de sanctions, de préserver la réputation de l'organisme et de démontrer une posture de coopération et de maîtrise réglementaire.

Quoi	**Qui**
44 – En cas d'intervention d'une personne en charge du contrôle, installer l'examinateur dans une salle de réunion, et prévenir immédiatement le DPO	Accueil – Tout collaborateur
45 – Contacter immédiatement votre conseil	DPO
46 – Prise de note de toutes les réponses formulées et réponses transmises	DPO
47- Ne pas laisser, pour des questions de sécurité, un examinateur, sans la présence d'un collaborateur	DPO
48- Ne jamais refuser la communication d'un document, mais en cas de doute, proposer la transmission du document sous quelques jours	DPO
49 – d'une manière générale, transmettre tout courrier, email ou notification provenant de la CNIL à son conseil	DPO

5. ARRIVEE ET DEPART DES COLLABORATEURS – POINTS DE VIGILANCES :

5.1. Procédure lors de l'arrivée d'un nouveau collaborateur

Lors de son arrivée, tout nouveau collaborateur doit recevoir :

- Une formation sur le RGPD
- La charte informatique
- La politique Données Personnelles Collaborateurs
- La présente procédure.

Ces éléments garantissent sa sensibilisation aux règles de confidentialité et à la sécurité des données dès son intégration.

La DSI doit être informer en amont, afin de permettre de définir les habilitations requises.

Quoi	**Qui**
50– Remise des documents de la conformité au collaborateur	DPO – Service RH
51 – Gestion des habilitations	DPO – DSI - RH
52 – Formation – sensibilisation RGPD	DPO

5.2. Formation continue des collaborateurs sur les dispositions relatives aux données personnelles

Chaque salarié impliqué dans le traitement de données personnelles doit être sensibilisé aux principes clés du règlement : licéité, minimisation, sécurité et droits des personnes. Cette formation permet de réduire les risques de violation, d'assurer une culture de la confidentialité, et de démontrer à la CNIL une démarche proactive de responsabilisation (accountability).

La formation des collaborateurs au RGPD doit être réalisée une fois par an, ou tous les deux ans selon leur niveau d'implication dans le traitement des données personnelles. Il est essentiel de documenter cette démarche et de conserver une trace des formations réalisées (dates, contenus, participants) afin de pouvoir démontrer la conformité en cas de contrôle.

Quoi	Qui
53– Formation – sensibilisation données personnelles 1 fois par an/ tous les deux ans	DPO – Service RH

5.3. Changement de poste d'un collaborateur ou départ d'un collaborateur :

La principale difficulté résulte dans le maintien d'habilitation qui n'ont plus lieur.

Par ailleurs, en cas de départ (ou de changement de poste), il convient de s'assurer de récupérer l'ensemble des outils mis à sa disposition

Quoi	Qui
54– Vérification et mise à jour des habilitations	DPO – Service RH – DSI
55 – Récupération des outils mis à disposition du collaborateur	DPO – Service RH – DSI

6. L'ARCHIVAGE DES DOCUMENTS ET LEUR MISE A JOUR

Il est nécessaire de conserver les documents suivants et de les regrouper dans un fichier attitré :

- Les politiques données personnelles
- Le registre des traitements
- Les analyses d'impact (AIPD) pour les traitements à risque
- Les contrats avec les sous-traitants et les clauses de responsabilité
- Les contrats avec les co-traitants
- Les registre des Droits
- Les registres des Violations
- Le Registre des Prestataires
- La Synthèse de mise en conformité
- Les preuves de formation des équipes : attestations de participation, supports de formation, feuilles d'émargement….
- Les factures ou conventions d'accompagnement juridique : elles attestent que l'association AXELERA a fait appel à un avocat pour sécuriser sa mise en conformité.
- Les notices d'information diffusées

- Les modèles de consentement : formulaires signés, logs de consentement en ligne, ou preuves d'acceptation explicite. Ces éléments sont cruciaux lorsque le traitement repose sur cette base légale.
- Les autorisations de droit à l'image
- Les différents échanges avec les DPD d'autres sociétés
- Les mentions sur les formulaires de collecte
- Les preuves de purge ou d'archivage : journaux d'effacement, rapports d'anonymisation, ou attestations de suppression par les prestataires.

Ces documents doivent être datés, et la date de dernière modification doit apparaitre.

Une revue de ces documents, à chaque nouveau traitement et au moins deux fois par an est requis.

La traçabilité est essentielle pour prouver que les droits des personnes sont respectés, que les données sont sécurisées, et que les traitements sont maîtrisés. En cas de contrôle de la CNIL, cette documentation est la première ligne de défense.

Quoi	**Qui**
56– Vérification et mise à jour de l'ensemble des documents de la conformité	DPO – Assistant à DPO