AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES
(APDP)

FORMATION DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES PERSONNELLES

Thème : *les notions de finalités des traitements et la cartographie des traitements*

Intervenant : Professeur ZANNOU Martial Tiburce

Novembre 2021

Sommaire

I. Notion de finalité, definition, utilité et distinctions

- **La finalité du traitement** est l'objectif principal de l'utilisation de données personnelles. Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.

- Un traitement de données est toute opération qui porte sur des données à caractère personnel, quel que soit le procédé, le support utilisé, informatisé ou non. Les données sont utilisées pour répondre à des objectifs/des finalités. Le traitement de données au sens de la « protection des données à caractère personnel » dépasse l’analyse ou l’exploitation de la donnée, il concerne la collecte, l’analyse, la réutilisation des données, l’archivage

- Exemple : L’hébergement de données sont des traitements de données personnelles.

A.Definition et utilité

- La finalité du traitement fait partie des principes essentiels de la règlementation. Tout traitement de données se réalise en fonction d’une finalité déterminée, explicite et légitime.
- La finalité d’un traitement de données personnelles est le pourquoi, l’objectif de l’action qui a été mise en place sur des données personnelles.

1. Sens et types de finalités

- Cet objectif doit être rédigé de façon très précise : on parle de finalité déterminée et explicite.
- La finalité doit être ***déterminée, légitime et explicite***:
  - L’objectif doit être légitime, c’est-à-dire respecter le cadre légal en vigueur et ne doit pas être modifié par la suite (on parle alors de détournement de finalité).

- L’objectif poursuivi par la mise en place du fichier doit être **compatible** avec les missions de l’organisme,
- Il doit être ***clair et compréhensible.***
- La finalité doit être définie précisément avant toute mise en œuvre d’un traitement de données personnelles.
- Si la finalité doit évoluer, cette évolution doit être opérée en toute transparence envers les personnes concernées et dans le respect de leurs droits (consultation, modification, suppression, opposition). Le responsable de traitement doit recueillir le consentement des personnes pour ce nouvel objectif.

2. Utilité et enjeux liés

- La finalité indique à quoi le fichier va servir. Lorsqu’un fichier est inscrit dans le registre des activités de traitement, sa finalité doit être évoqué » : cette finalité devra être respectée tout au long de la construction et de l'utilisation du dit. fichier.
- Exemples de finalités : gestion du recrutement, gestion de la clientèle, enquête de satisfaction, protection des biens et des personnes, etc.

- ***La finalité doit être respectée***
-
- Par exemple, un fichier de recrutement ne peut pas être utilisé pour proposer des offres commerciales aux candidats à un emploi dans votre société.
- La finalité permet de déterminer la pertinence des données personnelles que vous recueillez
- Seules les données adéquates et strictement nécessaires pour atteindre la finalité de votre fichier sont autorisées à y figurer.

- Par exemple, il n'est pas pertinent de demander le numéro de sécurité sociale d'un client pour alimenter un fichier dont la finalité est la gestion des achats d’un magasin de meubles.
- La finalité permet de fixer la durée de conservation des données du fichier
- En fonction du but poursuivi, les informations enregistrées dans le fichier pourront être conservées plus ou moins longtemps.
- Par exemple, lorsqu'un adhérent quitte une association, ses données doivent être supprimées du fichier de gestion des membres de l’association.

La cartographie

Afin de se mettre en conformité avec le code du numérique et pouvoir, notamment, tenir la documentation nécessaire à la bonne gestion des risques, chaque entreprise devra commencer par faire un inventaire des traitements des données à caractère personnel qu'elle collecte et / ou traite.

Une « cartographie des traitements » devra être réalisée et permettra d'identifier les actions à mener en interne pour être conforme au Règlement. Par ailleurs, si lors de cet inventaire la société constate que les traitements effectués comportent des risques pour les droits et libertés des personnes, elle devra réaliser une analyse d'impact et, dans certains cas, consulter l'autorité compétente

A/ Cartographie des traitements

Pour parvenir à cartographier les traitements réalisés par la société, il est nécessaire de recenser :

- les différents traitements de données personnelles mis en œuvre au sein de l'entreprise concernée ;
- le type de données personnelles traitées ;
- les objectifs poursuivis par le traitement ;
- les acteurs internes et externes (sous-traitants) qui s'occupent de ce traitement
- le lieu où les données collectées sont hébergées ;
- la durée de leur conservation ;

- les mesures de sécurité prises pour minimiser les risques ;
- ou encore le transfert des données, notamment hors Union européenne, s’il y a lieu.
- Identifier les actions à mener pour se conformer au Règlement16

Après avoir procédé à la cartographie des traitements des données, l’entreprise doit porter une attention particulière à ce que seules soient collectées et traitées les données strictement nécessaires à la poursuite de ses objectifs et être vigilante :

- au respect des modalités d’information prévues par le Règlement (informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée, informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée…)
- au respect des modalités d’exercice des droits des personnes concernées (accès, rectification, portabilité, suppression…) ;
- aux mesures de sécurité mises en place ;
- au respect de ses obligations par le sous-traitant (clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées).

B. Réalisation d'une étude d'impact relative à la protection des données pour les traitements à risque

Afin d'apprécier les risques sur la protection des données du point de vue des personnes concernées, la réalisation d'études d'impact pourra s'avérer nécessaire.

En effet, si le traitement des données collectées ou traitées est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable de traitement doit réaliser, avant le traitement, une analyse d'impact sur la vie privée. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Dans ce cas, le responsable de traitement demandera conseil au DPO, s'il y en a un.

Cette étude d'impact va, notamment, permettre d'évaluer l'origine, la nature et la gravité du risque, principalement en raison du contexte et de la finalité du traitement, et de mettre en place un traitement de données personnelles respectueux de la vie privée.

Elle doit être réalisée préalablement à la collecte des données personnelles et à la mise en œuvre du traitement de ces dernières et devra comprendre, notamment, les mesures, les garanties et les mécanismes envisagés pour atténuer ce risque.

Si cette étude d'impact indique que le traitement présenterait un risque élevé et si le responsable de traitement ne peut pas prendre de mesures appropriées pour atténuer le risque en raison des techniques disponibles et des coûts de mise en œuvre, une consultation préalable de l'autorité de contrôle devra être effectuée

Dans les cas où l’analyse d’impact est requise :

- « L’évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- le traitement à grande échelle de catégories particulières de données, ou de données à caractère personnel relatives à des condamnations pénales; ou
- la surveillance systématique à grande échelle d'une zone accessible au public ». L’autorité de contrôle pourra établir et publier une liste des types d’opérations de traitement pour lesquelles une analyse d’impact est ou non requise.
- L'analyse d’impact contient a minima :

  ♣ « une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;

  ♣ une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;

  ♣ une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et

  ♣ les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent Règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées ».

B-1) La tenue d'un registre des activités de traitement et d'une documentation interne

Le Règlement ayant pour but de responsabiliser les responsables de traitement, chaque société devra renforcer son dispositif contractuel, mettre en place une documentation interne et tenir également, dans certains cas, un registre des activités de traitement.

1.Mise en place d'un registre des activités de traitement

- Sauf exceptions, chaque responsable de traitement a l'obligation de tenir un registre des activités de traitement. Ce registre comporte les informations suivantes :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- les responsables des services opérationnels traitant les données au sein de l'entreprise ;
- les sous-traitants ;
- les catégories de données traitées ;
- les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé) ;
- les finalités pour lesquelles les données sont collectées ou traitées (ex : RH, gestion clients…) ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;
- le lieu où les données sont hébergées ou transférées et les documents attestant de l'existence de garanties appropriées ;
- les délais prévus pour l'effacement des différentes catégories de données (pendant combien de temps chaque catégorie de données est conservée) ;
- une description générale des mesures de sécurité mises en œuvre pour minimiser les risques d’accès non autorisés aux données. En cas de sous-traitance, le sous-traitant tiendra un registre de toutes les activités de traitement effectuées pour le compte du responsable de traitement. Ces registres se présentent sous une forme écrite, y compris la forme électronique, et doivent être tenus à la disposition de l'autorité de contrôle.

- Aux termes de l’article 428, lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

- Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

- L'analyse d'impact relative à la protection des données visée à l’alinéa 1er est, en particulier, requise dans les cas suivants :

- 1- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- 2- le traitement à grande échelle de catégories particulières de données visées à l'article 394, alinéa premier, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 395 ; ou
- 3- la surveillance systématique à grande échelle d'une zone accessible au public.
- L'Autorité établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément à l’alinéa 1er.
- L'Autorité peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

L'analyse contient au moins :

- 1- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- 2- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- 3- une évaluation des risques pour les droits et libertés des personnes concernées conformément à l’alinéa 1 ; et

4- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect des dispositions du présent Livre, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

- Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.
- Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

2/ ***Consultation préalable***

- Le responsable du traitement consulte l'Autorité préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article précédent indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

- Lorsque l'Autorité est d'avis que le traitement envisagé visé à l'alinéa 1er, constituerait une violation des dispositions du présent Livre, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'Autorité fournit par écrit, dans un délai maximum de huit (08) semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage de ses pouvoirs. Ce délai peut être prolongé de six (06) semaines, en fonction de la complexité du traitement envisagé. L'Autorité informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du

- délai ainsi que des motifs du retard, dans un délai de trente (30) jours à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que l'Autorité ait obtenu les informations qu'elle a demandées pour les besoins de la consultation.

- Lorsque le responsable du traitement consulte l'Autorité en application de l'alinéa 1er, il lui communique :

1- le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;

2- les finalités et les moyens du traitement envisagé ;

3- les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu des dispositions du présent Livre ;

4- le cas échéant, les coordonnées du délégué à la protection des données ;

5- l'analyse d'impact relative à la protection des données prévue à l'article précédent ; et

6- toute autre information que l'Autorité demande.

Merci pour votre aimable attention

Veuillez retrouver le présent slide : https://apdp.bj/formation-des-dpo-2021/

Pour plus de renseignements rendez-vous sur le site de l’APDP aux liens suivants :

- https://www.apdp.bj
- https://apdp.bj/les-outils-de-la-conformite/
- https://apdp.bj/procedures/