Certification HONCode
Formulaire d'auto-évaluation RGPD

La protection des données est l'utilisation juste et appropriée des informations personnelles

• Qu'est-ce que le RGPD ?

Le RGPD est le Règlement général sur la protection des données (UE) 2016/679. Il énonce les principes clés, les droits et les obligations pour la plupart des traitements de données à caractère personnel. Le RGPD est entré en vigueur le 25 mai 2018.

• Le RGPD me concerne-t-il ?

Le RGPD concerne :[1]

- les organisations situées dans l'UE
- les organisations situées en dehors de l'UE si elles offrent des biens ou des services aux personnes concernées de l'UE ou surveillent leur comportement.
- toutes les sociétés traitant et détenant les données personnelles des personnes concernées résidant dans l'Union Européenne, quel que soit le lieu où elles se trouvent.

• Qu'entend-on par "données à caractère personnel" ?[2]

En bref, les données personnelles sont des informations à propos d'une personne vivante. Il peut s'agir de n'importe qui, y compris un consommateur, un client, un employé, un partenaire, un membre, un sympathisant, un contact commercial, un fonctionnaire ou tout autre citoyen.

Il n'est pas nécessaire qu'il s'agisse d'informations "privées" - même des informations qui sont de notoriété publique ou qui concernent la vie professionnelle d'une personne peuvent être des données personnelles.

Les données à caractère personnel comprennent uniquement les informations relatives aux personnes physiques lorsque :

- elles peuvent être identifiées ou sont identifiables, directement à partir de l'information en question ; ou
- elles peuvent être identifiées indirectement à partir de cette information en combinaison avec d'autres informations.
- les données appartiennent à une catégorie particulière de données personnelles ou de données relatives aux condamnations pénales et aux infractions. Celles-ci sont

[1] https://eugdpr.org/the-regulation/gdpr-faqs/
[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

considérées comme plus sensibles et vous ne pouvez les traiter que dans des circonstances plus limitées.

Qu'est ce que le "traitement" ?[3]

Presque tout ce que vous faites avec des données est considéré comme un traitement, y compris la collecte, l'enregistrement, le stockage, l'utilisation, l'analyse, la combinaison, la divulgation ou la suppression.

• Qu'est-ce qu'un "contrôleur" ?

Le responsable du traitement est la personne qui décide comment et pourquoi collecter et utiliser les données. Il s'agit généralement d'une organisation, mais il peut s'agir d'une personne physique (par exemple, un entrepreneur individuel). Si vous êtes un employé agissant au nom de votre employeur, l'employeur serait le contrôleur. Le responsable du traitement doit s'assurer que le traitement de ces données est conforme à la loi sur la protection des données.

• Qu'est-ce qu'un "sous-traitant" ?

Un sous-traitant est une personne ou une organisation distincte (et non un employé) qui traite les données pour le compte du responsable du traitement et conformément à ses instructions. Les sous-traitants ont certaines obligations légales directes, mais celles-ci sont plus limitées que celles du responsable du traitement.

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/

FORMULAIRE D'AUTO-EVALUATION - INTRODUCTION

Le RGPD établit sept critères clés[4]

1. **Légalité, équité et transparence** : *Les données devraient être traitées de manière **licite, loyale et transparente** à l'égard des personnes.*
2. **Limitation de l'objectif :** *Les données devraient être collectées pour **des finalités déterminées, explicites et légitimes** et ne devraient pas être traitées ultérieurement d'une manière incompatible avec ces finalités.*
3. **Minimisation des données** : *La collecte des données devrait être **adéquate, pertinente et limitée** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.*
4. **Précision** : *Les données doivent être **exactes** et **à jour**.*
5. **Limitation du stockage** : *Les données ne devraient pas être conservées plus longtemps que **nécessaire**.*
6. **Intégrité et confidentialité** : *Les données devraient être traitées de manière à assurer une **sécurité appropriée** des données à caractère personnel.*
7. **Responsabilité** : *Le responsable du traitement est **responsable** de ces critères et est **en mesure d'en démontrer le respect**. Le responsable du traitement est la personne qui décide comment et pourquoi collecter et utiliser les données.*

Nous passerons en revue tous les principes, étape par étape, pour vous aider à vous assurer que vous respectez le RGPD, grâce à un formulaire.
N'hésitez pas à nous contacter si vous avez des questions sur ce règlement, notre équipe est à votre disposition pour vous aider.

FORMULAIRE D'AUTO-EVALUATION

Afin de vérifier si votre service est conforme au GDPR, nous allons passer en revue les 7 principes du Règlement.

Étape 1 – Déterminer votre droit de traiter des données personnelles

1. Quels sont vos critères d'admissibilité ?[5]

Vous devez déterminer votre admissibilité avant de pouvoir traiter des données personnelles. Au moins l'une d'entre elles devrait s'appliquer à votre service si vous traitez des données personnelles. Dans le cas contraire, vous n'êtes pas autorisé à traiter des données personnelles.

☐ **Consentement**[6]: la personne a donné son consentement clair pour que vous traitiez ses données personnelles à des fins spécifiques.

☐ Vous avez une demande de consentement distincte et compréhensible pour l'utilisation de votre service.

[4] https://gdpr-info.eu/art-5-gdpr/
[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
[6] https://gdpr-info.eu/art-7-gdpr/

☐ Vous avez un registre indiquant quand et comment vous avez obtenu le consentement de la personne.

☐ L'utilisateur a le droit de retirer son consentement à tout moment.

☐ Si votre entreprise a besoin d'un consentement pour offrir des services en ligne directement aux enfants, vous avez mis en place des systèmes pour les gérer.

Le consentement signifie offrir aux personnes un véritable choix et un contrôle sur la façon dont vous utilisez leurs données.

- Vous devez garder vos demandes de consentement bien en vue et les séparer des autres modalités et conditions.
- Proposez un opt-in positif tel que des cases d'opt-in décochées ou des méthodes d'opt-in actives similaires.
- Évitez de faire du consentement une condition préalable à l'usage du service.
- Soyez spécifique et granulaire. Permettez aux personnes de consentir séparément à différents objectifs et types de traitement, le cas échéant.
- Nommez votre entreprise et toute organisation tierce spécifique qui s'appuiera sur ce consentement.
- Conservez des dossiers sur ce à quoi une personne a consenti, y compris ce que vous lui avez dit, quand et comment elle a consenti.
- Dites aux personnes qu'elles peuvent retirer leur consentement en tout temps et comment le faire.[7]

Vous devez disposer d'une base légale pour traiter les données personnelles d'un enfant.

- Si vous offrez des services en ligne aux enfants, seul un enfant âgé de 13 ans ou plus sera en mesure de donner son propre consentement.
- Vous devrez donc faire des efforts raisonnables pour vérifier que toute personne donnant son propre consentement est suffisamment âgée pour le faire.
- Pour les enfants de moins de 13 ans, vous devez obtenir le consentement de la personne qui détient la responsabilité parentale de l'enfant.

☐ **Contrat :** le traitement est nécessaire pour un contrat que vous avez avec la personne ou parce qu'elle vous a demandé de prendre des mesures spécifiques avant de conclure un contrat.[8]

Vous vous fiez à cette base légale si vous devez traiter les données personnelles d'une personne : pour remplir vos obligations contractuelles envers elle ou parce qu'elle vous a demandé de faire quelque chose avant de conclure un contrat (par exemple fournir un devis).

☐ **Obligation légale** : le traitement est nécessaire pour vous permettre de vous conformer à la loi (sans compter les obligations contractuelles).

Vous vous fiez à cette base légale si vous devez traiter les données personnelles pour vous conformer à une obligation légale ou de droit commun.[9]

☐ **Intérêts vitaux :** le traitement est nécessaire pour protéger la vie d'une personne.

[7] https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/controllers-checklist/
[8] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/
[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/

Le traitement des données à caractère personnel devrait également être considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique. Le traitement de données à caractère personnel fondé sur l'intérêt vital d'une autre personne physique ne devrait en principe avoir lieu que lorsque le traitement ne peut être manifestement fondé sur une autre base juridique.[10]

☐ **Tâche publique :** le traitement est nécessaire à l'exécution d'une tâche d'intérêt public ou à l'exercice de vos fonctions officielles, et la tâche ou la fonction repose sur une base légale claire.

Vous pouvez vous prévaloir de cette base légale si vous devez traiter des données personnelles :

- « dans l'exercice de l'autorité publique ». Il s'agit des fonctions et pouvoirs publics prévus par la loi ;
- soit dans le cas d'accomplir une tâche particulière d'intérêt public prévue par la loi.

Elle s'applique surtout aux autorités publiques, mais elle peut s'appliquer à toute organisation qui exerce une autorité publique ou accomplit des tâches dans l'intérêt public.[11]

☐ **Intérêts légitimes :** le traitement est nécessaire aux fins de l'intérêt légitime poursuivi par le responsable du traitement ou par un tiers, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent la protection des données à caractère personnel ne l'emportent sur ces intérêts. (Ceci ne s'applique pas si vous êtes une autorité publique qui traite des données pour l'exécution de vos tâches officielles.)

Si vous choisissez de vous appuyer sur des intérêts légitimes, vous assumez une responsabilité supplémentaire dans la prise en compte et la protection des droits et des intérêts des personnes.

[10] https://gdpr-info.eu/recitals/no-46/
[11] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/

Étape 2 – Respecter les 7 critères du RGPD

Critère 1 - Légalité, équité et transparence

Les données devraient être traitées de manière licite, loyale et transparente à l'égard des personnes.[12]

Votre entreprise a déterminé votre éligibilité au traitement des données et l'a documenté.
Le premier principe exige que vous traitiez toutes les données personnelles légalement, équitablement et de manière transparente. Si aucune exigence légale pour le traitement, votre traitement sera illégal et en violation du premier principe.

☐ Oui
☐ Non

☐ Vous ne faites rien d'illégal avec des données personnelles (Légalité)

La légalité signifie également que vous ne faites rien avec les données personnelles qui est illégal dans un sens plus général. Cela comprend les obligations prévues par la loi qu'elles soient criminelles ou civiles. Si le traitement implique la réalisation d'une infraction pénale, il sera évidemment illicite.
Toutefois, le traitement peut également être illicite s'il aboutit à :

- une violation d'un devoir de confidentialité ;
- ce que votre organisation outrepasse ses pouvoirs légaux ou exerce ses pouvoirs de manière abusive ;
- une violation du droit d'auteur ;
- la violation d'une entente contractuelle exécutoire ;
- une infraction à une loi ou à un règlement propre à l'industrie ; ou
- une violation de la loi de 1998 sur les droits de l'homme.[13]

☐ Vous ne traitez les données des gens que de la manière à laquelle ils pourraient raisonnablement s'y attendre. (Équité)

Le principe de loyauté signifie que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. [14]
En général, l'équité signifie que vous ne devez traiter les données personnelles que d'une manière à laquelle les gens pourraient raisonnablement s'y attendre et ne pas les utiliser d'une manière qui aurait des effets négatifs et injustifiés sur ces personnes. Vous devez réfléchir non seulement à la manière dont vous pouvez utiliser vos données personnelles, mais aussi à la question de savoir si vous devez le faire.

☐ Vous respectez les obligations de transparence du droit à l'information.

Le principe de transparence exige que toute information et communication relative au traitement de ces données à caractère personnel soit facilement accessible et facile à comprendre, et que le langage utilisé soit clair et simple.

[12] https://gdpr-info.eu/art-5-gdpr/
[13] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/
[14] https://gdpr-info.eu/recitals/no-39/

Critère 2 - Limitation de l'objectif

Les données à caractère personnel sont : collectées pour des finalités déterminées, explicites et légitimes et ne font pas l'objet d'un traitement ultérieur incompatible avec ces finalités ; le traitement ultérieur à des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales.

☐ Vous avez clairement identifié la raison pour laquelle vous recueillez des données personnelles et ce que vous avez l'intention d'en faire.

Les finalités spécifiques pour lesquelles les données à caractère personnel sont traitées devraient être explicites et légitimes et déterminées au moment de la collecte des données à caractère personnel.

☐ Vous précisez ces fins dans une politique de confidentialité appropriée et compréhensible pour les particuliers.

Si vous envisagez d'utiliser des données personnelles pour une nouvelle finalité, vous devez vérifier que celle-ci est compatible avec votre finalité initiale ou obtenir un consentement spécifique pour cette nouvelle finalité. [15]

Critère 3 – Minimisation des données

Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire aux finalités pour lesquelles elles sont traitées.[16]

☐ Vous ne recueillez que les données personnelles dont vous avez réellement besoin à des fins spécifiques. (Pertinent)

☐ Vous disposez de suffisamment de données personnelles pour réaliser correctement ces objectifs. (Adéquat)

☐ Vous révisez périodiquement les données que vous détenez et supprimez tout ce dont vous n'avez pas besoin. (Limité)

Cela implique, en particulier, de veiller à ce que la durée de conservation des données à caractère personnel soit limitée au strict minimum. Afin de garantir que les données à caractère personnel ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour l'effacement ou pour un réexamen périodique.[17]

Critère 4 - Précision

Les données à caractère personnel doivent être exactes et, le cas échéant, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans délai.

☐ Vous vous assurez que les données personnelles que vous détenez sont exactes et à jour et de toutes les données personnelles que vous créez.

[15] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/
[16] https://gdpr-info.eu/art-5-gdpr/
[17] https://gdpr-info.eu/recitals/no-39/

Toutes les mesures raisonnables devraient être prises pour faire en sorte que les données à caractère personnel inexactes soient rectifiées ou effacées.
En pratique, cela signifie que vous devez :

- prendre des mesures raisonnables pour assurer l'exactitude des données personnelles ;
- vous assurer que la source et le statut des données personnelles sont clairs ;
- examiner attentivement toute contestation de l'exactitude de l'information ; et
- déterminer s'il est nécessaire de mettre à jour périodiquement l'information.

Critère 5 - Limitation du stockage

Les données à caractère personnel sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées plus longtemps dans la mesure où elles sont traitées uniquement à des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, à condition que soient prises les mesures techniques et organisationnelles requises par le présent règlement afin de sauvegarder les droits et libertés des personnes concernées ("limitation du stockage")

☐ Vous ne conservez pas les données personnelles plus longtemps que nécessaire.

Même si vous recueillez et utilisez les données personnelles de manière honnête et légale, vous ne pouvez pas les conserver plus longtemps que vous n'en avez réellement besoin. En plus de vous aider à respecter les principes de minimisation et d'exactitude des données, cela réduit également le risque que vous utilisiez ces données par erreur - au détriment de toutes les personnes concernées.[18]

☐ Vous avez établi et documenté des délais de conservation standard pour les différentes catégories d'informations que vous détenez, dans la mesure du possible.

Afin de garantir que les données à caractère personnel ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour l'effacement ou pour un réexamen périodique.[19]

Critère 6 - Intégrité et confidentialité (Sécurité)

Les données à caractère personnel devraient être traitées de manière à assurer une sécurité appropriée des données à caractère personnel, y compris la protection contre tout traitement non autorisé ou illicite et contre toute perte, destruction ou détérioration accidentelle, par des mesures techniques ou organisationnelles appropriées.[20]

☐ Vous traitez les données personnelles d'une manière qui assure une sécurité appropriée pour éviter que les données personnelles que vous détenez ne soient accidentellement ou délibérément compromises.

Afin de maintenir la sécurité et d'empêcher tout traitement contraire au présent règlement, le responsable du traitement ou le sous-traitant devrait évaluer les risques

[18] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/
[19] https://gdpr-info.eu/recitals/no-39/
[20] https://gdpr-info.eu/art-5-gdpr/

inhérents au traitement et mettre en œuvre des mesures visant à atténuer ces risques, telles que le cryptage.

Ces mesures devraient garantir un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état de la technique et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger.[21]

☐ Vous utilisez le cryptage et/ou la pseudonymisation lorsqu'il est approprié de le faire.

Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au risque, notamment, le cas échéant, la pseudonymisation et le cryptage des données à caractère personnel.[22]

☐ En cas d'atteinte à la protection des données, nous avertissons, dans un langage clair et compréhensible, l'autorité de contrôle dans les 72 heures et les utilisateurs sans retard injustifié.

Par conséquent, dès que le responsable du traitement a connaissance d'une violation des données à caractère personnel, il doit notifier cette violation à l'autorité de contrôle sans retard injustifié et, si possible, au plus tard 72 heures après en avoir eu connaissance.[23]

Le responsable du traitement devrait communiquer sans retard injustifié à la personne concernée toute violation de données à caractère personnel susceptible d'entraîner un risque élevé pour les droits et libertés de la personne physique, afin de lui permettre de prendre les précautions nécessaires.[24]

Critère 7 - Responsabilité

Le responsable du traitement est responsable des principes antérieurs et est en mesure d'en démontrer le respect.

☐ Vous assumez la responsabilité de vous conformer au RGPD et révisez vos mesures de reddition de comptes à des intervalles appropriés.

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, plus ou moins probables et graves, auxquels sont exposés les droits et libertés des personnes physiques, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir et démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et mises à jour si nécessaire.[25]

[21] https://gdpr-info.eu/recitals/no-83/
[22] https://gdpr-info.eu/art-32-gdpr/
[23] https://gdpr-info.eu/recitals/no-85/
[24] https://gdpr-info.eu/recitals/no-86/
[25] https://gdpr-info.eu/art-24-gdpr/

Étape 3 – Dernière Étape – 8 Droits des particuliers

1- Droit d'être informé

☐ Vous fournissez toutes les informations nécessaires sur votre organisation et les données personnelles que vous recueillez, dans votre Politique de confidentialité.

Plus de détails sur les informations que vous devez fournir : https://gdpr-info.eu/art-13-gdpr/

2- Droit d'accès

☐ Vous pouvez répondre aux demandes d'accès aux données personnelles des individus.

La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant font ou non l'objet d'un traitement et, le cas échéant, l'accès à ces données.[26]

3- Droit de rectification

☐ Vous respectez le droit de l'individu à la rectification sans délai injustifié et examinez attentivement toute contestation quant à l'exactitude des données personnelles.

N'oubliez pas que les personnes ont le droit absolu de faire rectifier les données à caractère personnel inexactes.

La personne concernée a le droit d'obtenir du responsable du traitement, sans retard injustifié, la rectification de données à caractère personnel inexactes la concernant. Compte tenu des finalités du traitement, la personne concernée a le droit de faire compléter les données à caractère personnel incomplètes, y compris en fournissant une déclaration complémentaire.[27]

4- Droit à l'effacement / Droit à l'oubli

☐ Vous avez mis en place des procédures appropriées pour donner suite aux demandes d'effacement présentées par des particuliers au titre du " droit d'être oublié ".

L'utilisateur a le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel le concernant sans retard injustifié et le responsable du traitement a l'obligation d'effacer ces données sans retard injustifié.[28]

5- Droit à la limitation du traitement

☐ Vous pouvez répondre à la demande d'une personne de restreindre le traitement de ses données personnelles.

La personne concernée a le droit d'obtenir du responsable du traitement une limitation du traitement. La personne concernée qui a obtenu une limitation du traitement est informée par le responsable du traitement avant que la limitation du traitement ne soit levée.[29]

6- Droit à la portabilité des données

☐ Vous disposez de processus permettant aux personnes de déplacer, copier ou transférer leurs données personnelles d'un environnement informatique à un autre d'une manière sûre et sécurisée, sans entrave à son utilisabilité.

La personne concernée devrait être autorisée à recevoir les données à caractère personnel la concernant qu'elle a fournies à un responsable du traitement dans un format

[26] https://gdpr-info.eu/art-15-gdpr/
[27] https://gdpr-info.eu/art-16-gdpr/
[28] https://gdpr-info.eu/art-17-gdpr/
[29] https://gdpr-info.eu/art-18-gdpr/

structuré, d'utilisation courante, lisible par machine et interopérable, et à les transmettre à un autre responsable du traitement.[30]

7- Droit d'opposition

☐ Vous disposez de moyens appropriés pour effacer, supprimer ou cesser de toute autre manière le traitement des données personnelles, sur le droit d'opposition de l'utilisateur.

Lorsque le traitement de données à caractère personnel peut être licitement effectué parce que le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public ou dans l'exercice de l'autorité publique dont est investi le responsable du traitement, ou pour des motifs d'intérêt légitime d'un responsable du traitement ou d'un tiers, la personne concernée devrait néanmoins pouvoir s'opposer au traitement des données à caractère personnel relatives à sa situation particulière.[31]

8- Droit de porter plainte

☐ Vous avez pris des mesures telles que la mise à disposition d'un formulaire de dépôt de plainte, afin que vos utilisateurs puissent déposer une plainte auprès d'une autorité de contrôle.

Sans préjudice de tout autre recours administratif ou judiciaire, toute personne concernée a le droit de saisir une autorité de contrôle, notamment dans l'État membre de sa résidence habituelle, de son lieu de travail ou du lieu de l'infraction alléguée, si elle estime que le traitement de données à caractère personnel la concernant viole ce règlement.[32]

DPO : Délégué à la protection des données

☐ Vous êtes une autorité publique (à l'exception des tribunaux agissant dans l'exercice de leurs fonctions judiciaires);

☐ Vous effectuez un suivi régulier et systématique à grande échelle des individus (ex : suivi comportemental en ligne);

☐ Vous effectuez des traitements à grande échelle de catégories particulières de données ou de données relatives aux condamnations pénales et aux infractions.

☐ Aucune de ces propositions

Vous pouvez trouver utile de désigner un DPR sur une base volontaire même lorsque le RGPD ne vous y oblige pas.[33]

Si vous avez coché une des trois premières cases :

Recommandation du DPD : Vous devriez désigner un délégué à la protection des données, une personne ayant une connaissance approfondie de la législation et des pratiques en matière de protection des données devrait aider le responsable du traitement ou le sous-traitant à contrôler le respect interne du présent règlement.[34]

[30] https://gdpr-info.eu/recitals/no-68/
[31] https://gdpr-info.eu/recitals/no-69/
[32] https://gdpr-info.eu/art-77-gdpr/
[33] https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/controllers-checklist/
[34] https://gdpr-info.eu/recitals/no-97/

EIPD : Évaluations d'impact sur la protection des données

☐ Vous utilisez une évaluation systématique et approfondie des aspects de la personnalité des personnes physiques qui est fondée sur un traitement automatisé, y compris le profilage, et sur laquelle se fondent les décisions qui produisent des effets juridiques concernant la personne physique ou qui affectent les personnes physiques de manière similaire de manière significative ;

☐ Vous traitez à grande échelle des données relatives à des catégories spéciales ou à des infractions pénales ;

☐ Vous surveillez systématiquement et à grande échelle les lieux accessibles au public ;

☐ Aucune de ces propositions

Si vous avez coché une des trois premières cases :

Recommandation EIPD : Dans de tels cas, une évaluation de l'impact sur la protection des données devrait être effectuée par le responsable du traitement avant le traitement afin d'évaluer la probabilité et la gravité particulières du risque élevé, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque. Cette analyse d'impact devrait comprendre, en particulier, les mesures, garanties et mécanismes envisagés pour atténuer ce risque, assurer la protection des données à caractère personnel et démontrer le respect du présent règlement.