HACA PARTNERS
Audit & Governance

Certification "GDPR CARPA"

Conférence de la Chambre de Commerce à l'occasion des 5 ans de l'entrée en vigueur du RGPD

24 avril 2023

Agenda

- Certification RGPD, de quoi parle-t-on exactement ?
- Pourquoi se faire certifier ?
- Quels sont les avantages de la certification ?
- Une certification RGPD, comment ça marche ?
- A qui s'adresse la certification ?
- Conclusion

Certification RGPD
de quoi parle-t-on exactement ?

CNPD

- En 2022, la Commission Nationale pour la Protection des Données (CNPD) devenait **la première autorité de protection des données en Europe** à adopter un système de certification Règlement Général pour la Protection des Données (RGPD).
- Une certification RGPD permet aux entreprises, institutions et organismes basés au Luxembourg de **démontrer la conformité RGPD de leur processus** vis-à-vis de l'ensemble de leurs parties prenantes : clients, partenaires, régulateurs, etc.
- La CNPD a laissé l'opportunité de l'article 42 du RGPD aux entités sous sa responsabilité de faire certifier processus spécifiques de protection des données pour les contrôleurs de données et les processeurs de données sur la base du schéma de certification CARPA.

Certification RGPD
de quoi parle-t-on exactement ?

RGPD – “CARPA”

- La CNPD a adopté les critères de certification GDPR-CARPA le 13 mai 2022. GDPR-CARPA est le premier schéma de certification sous le RGPD au niveau national et international.

- La certification se base sur la norme ISAE 3000 (International Standard on Assurance Engagements) mais aussi SCQ1 (contrôle qualité des organismes d’audit) et le standard ISO 17065 (accréditation d’organismes de certification). Ces critères d’agrément encadrent les travaux effectués par l'organisme de certification et le professionnel de l'audit.

- Le rapport ISAE se fait sous la forme d’un rapport ISAE 3000 Type 2 qui permet d’émettre une opinion sur la conception du dispositif précité et la bonne mise en œuvre de ce dispositif de contrôle dans la durée.

Pourquoi se faire certifier?

Au cœur de tous les arguments,
la confiance !

- En effet, une certification RGPD apporte à vos clients et partenaires l'assurance que les données personnelles qui vous sont confiées sont en sécurité avec vous.
- Tout Responsable de Traitement se doit d'obtenir une garantie de la part de ses sous-traitants que les données confiées sont protégées et sécurisées. Être un sous-traitant dont les processus sont certifiés permet de montrer patte blanche et de démontrer de facto une conformité au RGPD.
- Ainsi, ce sont les différents acteurs de la chaîne de valeur qui exigent souvent que leurs partenaires de cette même chaîne soient en mesure de démontrer un niveau suffisant de conformité au RGPD.
- Pierre angulaire des relations d'affaires, la confiance apportée par la certification constitue donc un élément appréciable à l'ère de la digitalisation et des risques croissants qu'elle amène dans son sillage.

Pourquoi se faire certifier?

Si vous pensez que la mise en conformité RGPD coûte cher, la non-conformité pourrait se révéler bien plus coûteuse

- Dans un monde où la protection des données est un enjeu majeur pour tous les acteurs, pouvoir démontrer la conformité de ses processus de traitement au RGPD devient un argument commercial qui fait la différence pour les partenaires économiques des entités certifiées.
- Son importance au niveau de la gouvernance interne ne va faire que croître au fur et à mesure du développement de la cybercriminalité et de la multiplication des amendes infligées par les autorités de contrôles
- Des sanctions peuvent s'élever jusqu'à 20 millions € ou jusqu'4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. A noter qu'avec une amende de 746 millions d'euros à Amazon, la CNPD est l'autorité de contrôle européenne ayant infligé l'amende la plus élevée pour violation du RGPD à notre connaissance

Quels sont les avantages de la certification?

De multiples avantages

+

- **Apporter l'assurance de la conformité réglementaire** des traitements visés par la certification ;
- Assurer la **base de confiance** nécessaire au développement **d'une relation d'affaires** ;
- Nourrir et renforcer **la réputation** de l'entité dont les processus sont certifiés ;
- Apporter l'assurance **d'un engagement d'amélioration continue** car si la durée de validité d'un certificat est de 3 ans, la certification n'est confirmée que sous réserve d'un audit complet annuel réussi ;
- Constituer un **avantage commercial de taille et Se prémunir** contre les amendes des autorités de contrôle.

Quels sont les avantages de la certification?

Image de la société certifiée

- Outre ce dernier bénéfice, les autres avantages **sont autant d'arguments marketing** qui sont de nature à offrir aux entités certifiées des nouvelles opportunités de développement. En effet, si tous les acteurs déclarent traiter vos données avec intégrité et confidentialité en respectant les réglementations, cette assertion sans contrôle ne peut totalement convaincre.

- Avec une certification, vous disposez d'un document audité par un professionnel externe indépendant vous donnant un **sceau d'approbation tiers**, établi selon une nome reconnue internationalement.

Processus d'audit en pratique

Processus d'agréement

- Le processus d'agréement auprès de la CNPD est un processus minutieux qui demande une mise en place de procédures et de plans de contrôles en amont de la demande d'agréement.
- Les procédures à mettre en place couvrent à la fois des manuels d'assurance qualité, des chartes d'objectivité et d'indépendance, mais aussi des plans de formation, des registres de traitement des données, …
- Le cabinet doit aussi expliquer les plans de contrôles par toutes les équipes étant impliquées sur les dossiers, y compris le processus d'audit interne du cabinet

Processus d'audit en pratique

Un processus de revue continue

- Au niveau du cabinet, il y aura 4 équipes qui devront travailler de façon indépendante:
  - L'équipe dite d'évaluation: Equipe « terrain » qui va évaluer la conformité des processus et faire des tests de détails
  - L'équipe dite de certification: Equipe qui va être en charge de la certification finale du rapport. Le réviseur d'entreprises en charge de ce rapport et la signature de ce dernier fera partie de cette équipe. Les membres de cette équipe ne peuvent avoir fait partie de l'équipe d'évaluation
  - L'équipe dite de revue qualité menée par un réviseur d'entreprises: Chaque mission fera l'objet d'une mission de revue qualité par une équipe menée par un réviseur d'entreprises. Aucun des membres n'aura pu participer à des travaux dans une des autres équipes.
  - L'équipe dite d'audit interne: de façon annuelle (pluri-annuelle?) le processus global du cabinet sera revu par une équipe indépendante d'audit interne et fera des échantillonnages de mission
- De plus, la CNPD fera une revue périodique du revue du cabinet et fera des échantillonnages de mission

Processus d'audit en pratique

Pour les entreprises de toute taille et de tout secteur

- La certification est pertinente pour les entreprises de toute taille et de tout secteur qui souhaitent adopter les meilleurs pratiques ou répondre aux exigences de leur chaîne de valeurs.
- On notera que la certification convient particulièrement aux entreprises qui fournissent des services externalisés, qui traitent des données sensibles (données de santé, par exemple) ou en large quantité (services publics entre autres).

Processus d'audit en pratique

Et en particulier, les secteurs:

- Aux acteurs du secteur de la gestion d'actifs (gestionnaire de fonds d'investissement, banque dépositaire, agent teneur de registres, etc.),
- Au secteur public et ses nombreux opérateurs qui traitent des données personnelles de citoyens et se doivent d'être exemplaires,
- Aux opérateurs qui offrent des prestations de service en mode SaaS,
- Aux data centers,
- Aux entreprises qui internalisent des fonctions d'autres clients : gestion de la paie, fonctions comptables, prestations commerciales, etc.,
- Aux hôpitaux, gestionnaires et hébergeurs de données de santé,
- Aux opérateurs télécoms dont les informations de trafic et de localisation des téléphones mobiles constituent des données particulièrement sensibles pour le grand public,
- Aux entreprises qui ont pour modèle économique le commerce de données personnelles : location de bases de données, ciblage publicitaire, suivi et analyse de trafic sur internet.

Article AGEFI sur la certification RGPD mars 2023

Pourquoi une certification RGPD ?

En 2022, la Commission Nationale pour la Protection des Données (CNPD) devenait la première autorité de protection des données en Europe à adopter un système de certification Règlement Général pour la Protection des Données (RGPD). En février 2023, HACA PARTNERS devient le 2ème organisme certificateur RGPD accrédité par la CNPD.

Cabinet de révision agréé comptant plus de 60 collaborateurs, le premier atout d'HACA est l'agilité liée à sa taille. Mais cet avantage n'est pas des moindres. En effet, HACA PARTNERS n'a pas hésité à unir ses forces avec deux acteurs RGPD de la place : un cabinet d'avocat, DSM Avocats à la Cour, pour toutes les questions juridiques et Seralys une société spécialisée en sécurité informatique. Ce partenariat nous est paru d'autant plus naturel que les lignes bougent constamment en matière de protection des données et que cette coopération nous permet de garder une longueur d'avance sur tous les fronts de cette matière.

Certification RGPD, de quoi parle-t-on exactement ?

Une certification RGPD permet aux entreprises, institutions et organismes basés au Luxembourg, de **démontrer la conformité RGPD de leur processus** vis-à-vis de l'ensemble de leurs parties prenantes : clients, partenaires, régulateurs, etc.

La certification se base sur la norme ISAE 3000 (International Standard on Assurance Engagements). Il s'agit d'une norme d'assurance sur les informations non financières publiée par la Fédération internationale des professionnels de l'information financière (IFAC). Le rapport est un rapport de **contrôle interne** qui se concentre sur les contrôles en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité de l'information traitée. Plus simplement, il s'agit d'un sceau d'approbation par un auditeur ayant reçu l'agrément de certification RGPD indiquant que les processus certifiés assurent un traitement des données correct et conforme au RGPD. Au Luxembourg, la CNPD a fait le choix de réserver cette capacité de certification RGPD aux réviseurs d'entreprises agréés.

Dans un monde où la protection des données est un enjeu majeur pour tous les acteurs, pouvoir démontrer la conformité de ses processus de traitement au RGPD devient un **argument commercial** qui fait la différence pour les partenaires économiques des entités certifiées. Son importance au niveau de la gouvernance interne ne va faire que croître au fur et à mesure du développement de la cybercriminalité et de la multiplication des amendes infligées par les autorités de contrôles qui, on le rappelle, peuvent s'élever jusqu'à 20 millions € ou jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. A noter qu'avec une amende de 746 millions d'euros à Amazon, la CNPD est l'autorité de contrôle européenne ayant infligé l'amende la plus élevée pour violation du RGPD. Car si vous pensez que la mise en conformité RGPD coûte cher, la non-conformité pourrait se révéler bien plus coûteuse !

Pourquoi se faire certifier ?

Au cœur de tous les arguments, la **confiance** ! En effet, une certification RGPD apporte à vos clients et partenaires l'assurance que les données personnelles qui vous sont confiées sont en sécurité avec vous. Tout Responsable de Traitement se doit d'obtenir une garantie de la part de ses sous-traitants que les données confiées sont protégées et sécurisées. Être un sous-traitant dont les processus sont certifiés permet de montrer patte blanche et de démontrer *de facto* une conformité au RGPD. Ainsi, ce sont les différents acteurs de la chaîne de valeur qui exigent souvent que leurs partenaires de cette même chaîne soient en mesure de démontrer un niveau suffisant de conformité au RGPD. Pierre angulaire des relations d'affaires, la confiance apportée par la certification constitue donc un élément appréciable à l'ère de la digitalisation et des risques croissants qu'elle amène dans son sillage.

Quels sont les avantages de la certification ?

Les avantages de la certification sont nombreux. Parmi les plus importants, on citera :
#1 apporter l'**assurance de la conformité réglementaire** des traitements visés par la certification ;
#2 assurer la **base de confiance nécessaire au développement d'une relation d'affaires** ;
#3 nourrir et renforcer la **réputation** de l'entité dont les processus sont certifiés ;
#4 apporter l'assurance d'un **engagement d'amélioration continue** car si la durée de validité d'un certificat est de 3 ans, la certification n'est confirmée que sous réserve d'un audit complet annuel réussi ;
#5 constituer un **avantage commercial** de taille ;
#6 **se prémunir contre les amendes** des autorités de contrôle.

Outre ce dernier bénéfice, les autres avantages sont **autant d'arguments marketing** qui sont de nature à offrir aux entités certifiées des nouvelles opportunités de développement. En effet, si tous les acteurs déclarent traiter vos données avec intégrité et confidentialité en respectant les réglementations, cette assertion sans contrôle ne peut totalement convaincre. Avec une certification, vous disposez d'un document audité par un professionnel externe indépendant vous donnant **un sceau d'approbation tiers**, établi selon une norme reconnue internationalement.

Une certification RGPD, comment ça marche ?

Le schéma de certification de la CNPD repose sur la norme de travail internationale ISAE 3000 de type 2. La norme ISAE 3000 définit les missions d'assurance autres que celles relatives aux informations financières. C'est ce champ d'application très large qui admet une application dans le domaine de la protection des données et permet à des acteurs de démontrer leur conformité RGPD, grâce à l'émission d'une opinion par un auditeur, professionnel indépendant, agréé par la CNPD. Cette norme encadre toutes les missions de certification, dans lesquelles l'auditeur mesure ou évalue des process au regard de critères précis. Celui-ci cherchera à obtenir des éléments probants suffisants et appropriés en vue d'exprimer une conclusion visant à renforcer la confiance des parties prenantes quant au respect du RGPD. Le dispositif de conformité au RGPD n'est donc ni plus ni moins qu'un dispositif de contrôle interne appliqué aux données personnelles.

Dans la famille ISAE 3000, on distingue deux types de rapports :
- le type 1 qui permet d'émettre une opinion à un « instant T » : l'auditeur valide la bonne conception du dispositif de contrôle permettant de couvrir le risque de non-conformité ;
- le type 2 qui permet d'émettre une opinion sur la conception du dispositif précité **et** la bonne mise en œuvre de ce dispositif de contrôle dans la durée.

La CNPD a donc retenu le rapport ISAE 3000 de type 2 pour la certification RGPD. Dans le cadre de la certification RGPD, l'auditeur conduira deux types de travaux :
- Il va, tout d'abord, s'assurer de la conception et de la mise en œuvre de l'ensemble des mesures qui permettent de se conformer aux exigences du RGPD : mesures de gouvernance, opérationnelles, de sécurité de l'information et d'encadrement contractuel des relations avec les sous-traitants. L'auditeur sera ainsi en mesure de porter un avis sur la pertinence du dispositif de conformité mis en place.
- Dans un second temps, il s'assurera de l'efficacité opérationnelle du dispositif. Pour se faire il réalisera des tests afin de s'assurer que les procédures sont effectivement mises en œuvre au sein de l'organisation sur une période déterminée.

La norme ISAE 3000 garantit un niveau d'exigence important, facteur décisif pour que tous les acteurs - dont les personnes concernées - se sentent en confiance grâce à **l'assurance que les process sont opérés dans un cadre de contrôle interne pertinent (qui adresse les risques identifiés) et robuste (effectivement déployé et testé).**

On notera que, bien que des éléments de sécurité de l'information aient été intégrés dans le schéma, ils ne constituent pas le focus de ce mécanisme de certification.

A qui s'adresse la certification ?

La certification est pertinente pour les entreprises de toute taille et de tout secteur qui souhaitent adopter les meilleures pratiques ou répondre aux exigences de leur chaîne de valeurs. Ainsi, les critères de certification GDPR sont conçus de manière suffisamment flexibles afin d'être pertinents pour une panoplie d'opérations de traitement dans plusieurs secteurs. Chaque entité peut définir et mettre en œuvre les mesures qui conviennent le mieux à sa situation et à son secteur spécifique pour se conformer aux critères.

On notera que la certification convient particulièrement aux entreprises qui fournissent des services externalisés, qui traitent des données sensibles (données de santé, par exemple) ou en large quantité (services publics entre autres). On pensera ainsi en particulier aux :
- aux acteurs du secteur de la gestion d'actifs (gestionnaire de fonds d'investissement, banque dépositaire, agent teneur de registres, etc.),
- au secteur public et ses nombreux opérateurs qui traitent des données personnelles de citoyens et se doivent d'être exemplaires,
- aux opérateurs qui offrent des prestations de service en mode SaaS,
- aux data centers,
- aux entreprises qui internalisent des fonctions d'autres clients : gestion de la paie, fonctions comptables, prestations commerciales, etc.,
- aux hôpitaux, gestionnaires et hébergeurs de données de santé,
- aux opérateurs télécoms dont les informations de trafic et de localisation des téléphones mobiles constituent des données particulièrement sensibles pour le grand public,
- aux entreprises qui ont pour modèle économique le commerce de données personnelles : location de bases de données, ciblage publicitaire, suivi et analyse de trafic sur internet.

Conclusion

Toute organisation dont les processus sont certifiés RGPD envoie un message clair indiquant qu'elle traite les données avec intégrité, confidentialité et en conformité. Preuve de cette conformité, la certification permet ainsi de répondre aux préoccupations légitimes des parties prenantes en matière de protection des données et de sécurité de l'information et de rassurer tant les clients que les partenaires d'affaires et même leurs employés. La certification constitue pour eux l'assurance qu'une organisation maintient les normes de sécurité les plus élevées, évalue les risques en conséquence et effectue un excellent contrôle de la qualité du traitement des données. Un argument commercial de poids et une prévention contre des amendes de plus en plus nombreuses et importantes !

Laurence PONCHAUT (photo)
Senior Manager and Expert GDPR

Cyril CAYEZ (photo),
Co-founding Partner

Cédric LEROY
Partner – Head of Regulatory and Compliance

HACA Partners Sàrl
organisme certificateur accrédité par la CNPD

Pour en savoir plus, contactez lponchaut@hacapartners.lu, cleroy@hacapartners.lu ou ccayez@hacapartners.lu.

Laurence, Cédric et Cyril sont au sein de HACA Partners, cabinet de révision agréé, les responsables de ce service de certification RGPD attribué à HACA Partners par la CNPD. Actif en Regulatory & Compliance, en Risk Management, en Audit Interne et en Audit Externe par définition, HACA Partners réunit des professionnels expérimentés aptes à gérer ce service de certification de manière consciencieuse et efficace.

www.hacapartners.lu

Pour en savoir plus, contactez
lponchaut@hacapartners.lu
cleroy@hacapartners.lu ou
ccayez@hacapartners.lu

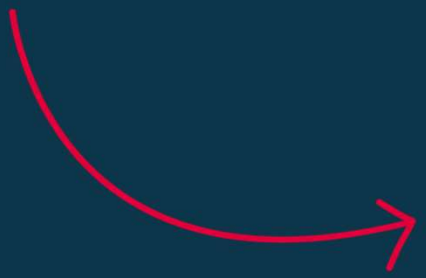
Conclusion

Toute organisation dont les processus sont certifiés RGPD envoie un message clair indiquant qu'elle traite les données avec intégrité, confidentialité et en conformité.

Preuve de cette conformité, la certification permet ainsi de répondre aux préoccupations légitimes des parties prenantes en matière de protection des données et de sécurité de l'information et de rassurer tant les clients que les partenaires d'affaires et même leurs employés. La certification constitue pour eux l'assurance qu'une organisation maintient les normes de sécurité les plus élevées, évalue les risques en conséquence et effectue un excellent contrôle de la qualité du traitement des données.

Un argument commercial de poids et une prévention contre des amendes de plus en plus nombreuses et importantes !

Merci de votre attention !



Avez-vous des questions?

www.hacapartners.lu