Grant Thornton

Les tendances d'évolution de la fonction de *DPO* dans les entreprises

Grant Thornton

Édito

Vers une transformation de la fonction *DPO* ?

La fonction de *DPO* (*Data Protection Officer*), est née il y a 4 ans avec le RGPD. Dès l'origine, les entreprises l'ont associée à la mise en conformité de ce règlement, avec une connotation très juridique ou liée aux systèmes d'information, en fonction des enjeux majeurs qui les animaient.

Depuis, le contexte a fortement évolué. Le RGPD, précurseur en Europe, a été rejoint par de nombreuses autres réglementations locales sur tous les autres continents. A ces réglementations sur la protection des données personnelles s'en sont ajoutées d'autres, plus générales, sur la *data*, l'intelligence artificielle, le *cloud*, chacune avec une incidence directe ou indirecte sur la gestion de la donnée personnelle.

Avec le RGPD, les entreprises se sont trouvées confrontées à une problématique : revisiter leurs activités sous la focale des données personnelles. Malheureusement, dans leur gestion quotidienne, cette distinction « donnée personnelle » et « donnée non personnelle » n'existait pas. En outre, elle peut parfois s'avérer particulièrement complexe, car une donnée non personnelle peut rentrer dans la catégorie des données personnelles en étant associée à d'autres données. De ce fait, la frontière entre les deux est parfois floue et peut amener à s'interroger sur la pertinence d'une telle distinction.

La conformité au RGPD est donc un sujet complexe, protéiforme, parfois très technique, tant sur des sujets juridiques que de sécurité des systèmes d'information. Face à cela, les *DPO*, en règle générale, ne disposent que de peu de moyens, et rarement à l'échelle des enjeux et du travail à accomplir.

Dans le même temps, les autorités de contrôle se sont organisées et sont maintenant en capacité de réaliser de nombreux contrôles et de prononcer des sanctions pouvant être particulièrement lourdes à l'encontre d'entreprises de tous les secteurs.

Enfin, les entreprises ont connu une explosion des violations de données depuis les périodes de confinement, sans distinction de taille ni de secteur d'activité.

Pour toutes ces raisons, faire un état des lieux de cette fonction nous a semblé nécessaire, afin de mieux comprendre les difficultés rencontrées, de connaître les principales réalisations de ses acteurs et les sujets qui restaient à traiter, et de voir comment elle évoluait au sein des organisations. Toutes nouvelles fonctions, surtout celles imposées par la réglementation, finissent par trouver leur place dans les organisations avec la maturité et la pratique. Souvent le point d'arrivée n'est pas celui d'origine.

Merci aux plus de 120 *DPO* qui ont participé à cette enquête, et à la quinzaine de *DPO* et d'éditeurs interviewés, pour la richesse de nos échanges.

Nous vous souhaitons une bonne lecture et espérons que ce voyage au sein de la profession de *DPO* sera riche d'enseignements et d'idées pour le futur.

Nicolas Gasnier-Duparc
Associé *Business Risk Services*,
En charge de l'offre *Data Privacy*
Grant Thornton

Nicolas Rémy-Néris
Avocat
DPO externalisé
Grant Thornton Société d'Avocats

Grant Thornton

Sommaire

Les tendances d'évolution de la fonction de *DPO* dans les entreprises

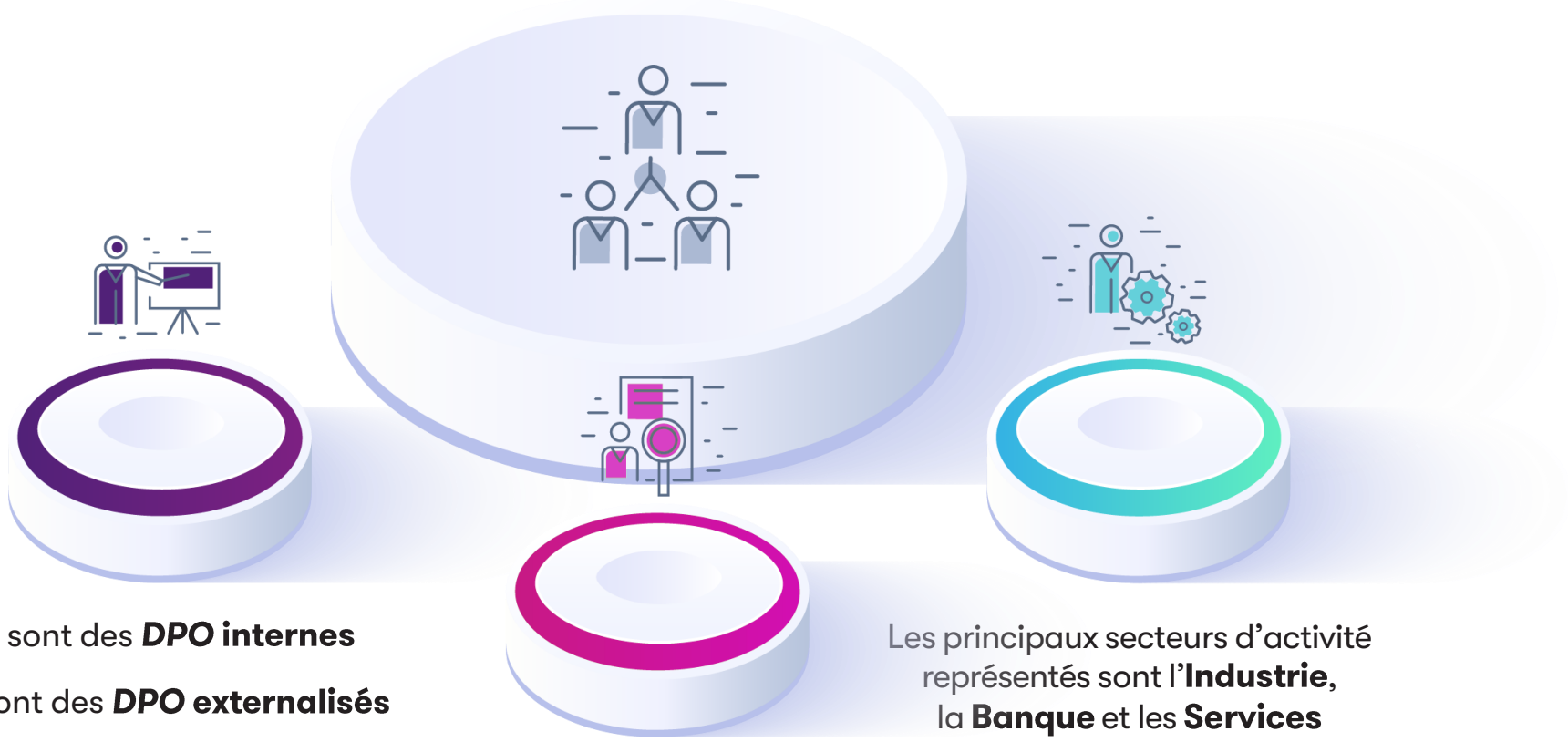
01 Présentation de l'échantillon

Grant Thornton

Une population représentative par sa diversité

Présentation de l'échantillon

Enquête réalisée par Grant Thornton auprès de 125 *DPO* internes et externes. Par questionnaire en ligne diffusé via les réseaux sociaux, complété avec certains entretiens ciblés entre les mois de mars et juin 2022.



2/3 sont des ***DPO* internes**

1/3 sont des ***DPO* externalisés**

Les principaux secteurs d'activité représentés sont l'**Industrie**, la **Banque** et les **Services**

Près de **70 %** d'entre eux exercent dans le secteur privé, et **30 %** dans le **secteur public**

02 Gouvernance

Grant Thornton

Gouvernance RGPD

Après quatre ans d'application du Règlement Général sur la Protection des Données, **la gouvernance** dédiée à la protection des données personnelles est devenue une clé de voûte des organisations et des entreprises, indispensable au bon déploiement et à la conformité au RGPD.

Pour la CNIL, la gouvernance en matière de traitement de données à caractère personnel se comprend comme « **l'ensemble des mesures, règles et bonnes pratiques** » **permettant la gestion** de ces données au sein d'une organisation. Cette démarche vise à intégrer les données personnelles dans la **stratégie**, les **objectifs** et la **conjoncture** de l'entreprise, afin d'assurer le respect de l'ensemble des principes du RGPD (sécurité informatique, juridique, etc.) dans son organisation.

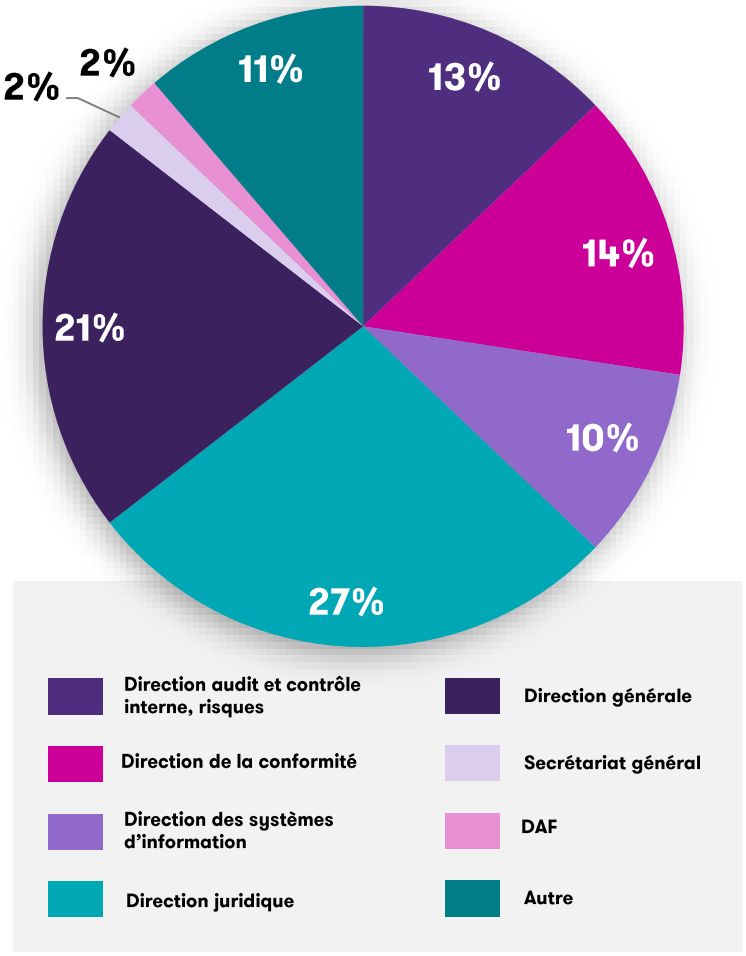
En pratique, la gouvernance de la donnée personnelle repose essentiellement **sur le triptyque humain, moyens techniques et moyens financiers**.

Le *DPO* est ainsi le chef d'orchestre de la mise en place du projet de gouvernance de l'entreprise ou de l'organisme en matière de RGPD.

Grant Thornton

Une redéfinition de son positionnement : des fonctions techniques vers la gestion des risques ...

A qui la fonction *DPO* est-elle rattachée dans votre organisation ?



« L'évolution du rattachement du DPO vers des fonctions de gestion des risques est probablement liée à une prise de conscience que ce sujet est aux côtés de la gestion des risques juridiques, également un sujet de gestion de risques opérationnels. Si des compétences juridiques et de systèmes d'information sont de fait nécessaires et essentielles à la fonction DPO, nous sommes chez Grant Thornton convaincus qu'il s'agit également d'un sujet de contrôle interne. »

Force est de constater que la fonction *DPO* a évolué depuis l'entrée en vigueur du Règlement Général sur la Protection des Données, tant sur son **rattachement hiérarchique** que sa **visibilité** au sein de l'entreprise, sans pour autant lui donner plus de **moyens**.

Alors qu'en 2018 **la fonction était principalement rattachée aux directions juridiques et systèmes d'information**, l'étude a montré que la situation se maintenait uniquement pour la direction juridique avec 27 % de *DPO* rattachés à cette dernière.

En 2022, 13 % ont déclaré être rattachés à **une direction des risques** (risques, audit et contrôle interne), et 21 % à la **direction générale**. En revanche, seulement 10 % restent rattachés à une direction informatique / systèmes d'information.

Enfin, 80 % (cf. annexe graphique N°1) des répondants se disent satisfaits de leur rattachement.
Après 4 ans, 42 % (cf. annexe graphique N°2) des répondants ont déclaré que leur **visibilité était bonne et suffisante au sein de l'entreprise,** contre 40 % (cf. annexe graphique N°2) qui considèrent que cette dernière doit être encore améliorée. Ce qui est notamment vrai pour les *DPO* rattachés aux « nouvelles directions » (risques et direction générale) qui estiment majoritairement ne pas avoir encore assez de visibilité en interne.

Ces évolutions tendent donc à démontrer qu'en 2022 la problématique des données personnelles est sortie du champ traditionnel juridique et informatique, pour s'inscrire dans une stratégie et gouvernance plus large de la donnée et des risques au sein des entreprises et des organismes.

Grant Thornton

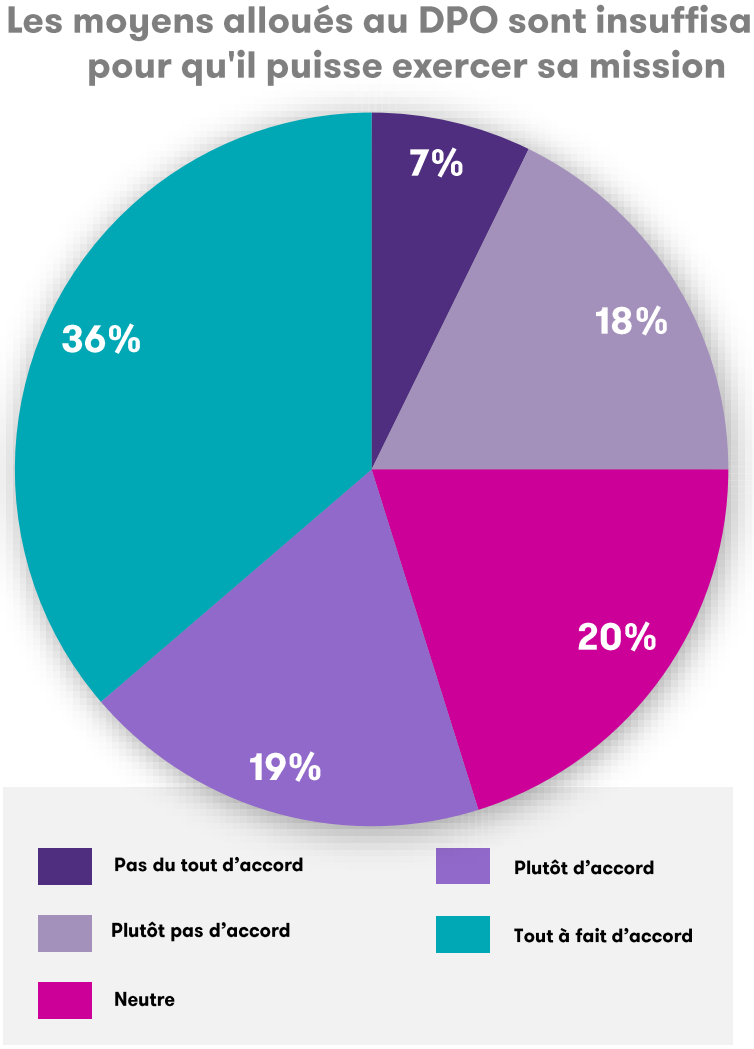
Une redéfinition de son positionnement : des fonctions techniques vers la gestion des risques...

« La part de gestion de projet et d'approche par les risques est de plus en plus grande pour les DPO. »

Aurélie Banck
DPO, Compliance Officer
Europcar Mobility Group

Grant Thornton

Mais avec peu de moyens !



Les moyens alloués au *DPO* sont insuffisants pour qu'il puisse exercer sa mission

En revanche, les **moyens alloués** au *DPO* stagnent depuis 2018. 55 % des répondants les trouvent **insuffisants.**

L'ampleur de la fonction de *DPO* est parfois sous-estimée, y compris au sein de grands groupes, tant sur son rôle, que sur sa responsabilité et ses missions. Avoir un *DPO* au sein de son organisation ne dispense pas cette dernière de lui donner des moyens pour exercer efficacement sa fonction.

Aussi, en fonction de son rattachement à une direction ou à une autre, l'on constate aujourd'hui que tous les *DPO* ne sont pas égaux concernant les moyens auxquels ils ont accès.

Notamment certaines directions, comme les DSI, mieux dotées budgétairement, permettent au *DPO* d'obtenir des ressources pour recruter ou investir dans des outils spécifiques. Cela n'est pas le cas pour les directions juridiques, ou de secrétariat général, ayant des budgets stables mais plutôt limités.

Grant Thornton

Mais avec peu de moyens !

Le DPO est un chef d'orchestre bien souvent avec un orchestre réduit ou pas d'orchestre.

Sarah Taïeb-Jaskierowicz
***Global DPO* UGI Group**

Les DPO sont sollicités sur tous les projets qui impliquent la collecte de données personnelles, c'est-à-dire sur pratiquement tout. Leur charge de travail est souvent importante, surtout lorsque le DPO n'intervient pas sur ces questions à temps plein. Mais la direction n'est malheureusement pas toujours consciente de cette charge.

Ola Mohty,
***DPO* chez Data Legal Drive**

Le rattachement du DPO dans l'organigramme a souvent un impact fort sur sa capacité à accéder à des budgets et à des moyens. Notamment historiquement, les DSI sont mieux dotées en la matière que les directions juridiques.

Me Franklin Brousse
Avocat et Associé fondateur de RGPD Check – Plateforme d'évaluation des sous-traitants

Le DPO est la clé de voûte de la conformité en matière de protection des données mais avec des moyens très limités au regard des enjeux.

Jennifer Godin
***DPO* du groupe ROQUETTE**

Grant Thornton

Et un réseau d'acteurs à consolider

Malgré une meilleure intégration dans la stratégie et la gouvernance de l'entreprise ou de l'organisme, le *DPO* a toujours des difficultés à embarquer les acteurs internes, qu'ils soient **stratégiques** ou **opérationnels,** dans une gouvernance efficiente.

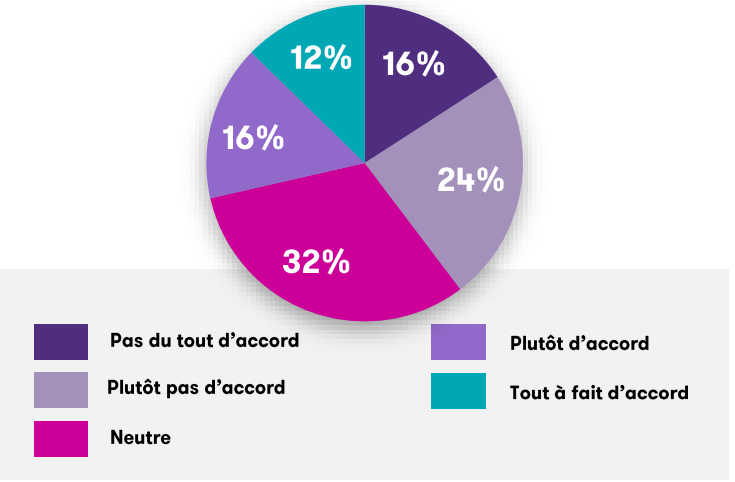
L'accessibilité et l'écoute de la direction générale sur les problématiques relatives à la protection des données demeurent **un enjeu non résolu** de la mise en place d'une gouvernance adéquate. En effet, seuls 40 % des répondants déclarent avoir un accès direct à la direction générale, quand 32 % évoquent des difficultés chroniques, mais sans impact majeur sur leurs activités de *DPO*. *A contrario*, 28 % affirment que le manque d'accès et d'écoute de la direction générale est un réel frein à la conduite de leurs missions.

Si en 2018, les *DPO* s'appuyaient largement sur les **acteurs externes** (cabinet de conseil, cabinet d'avocat, etc.), les compétences ont depuis été internalisées. 66 % des répondants s'appuient désormais sur une **équipe dédiée** ou sur un **réseau de correspondants** dans les directions métiers et fonctions supports pour la conduite de leurs missions. Cela a permis d'ancrer et de répartir la pluridisciplinarité des compétences de la fonction de *DPO* au sein des entreprises.

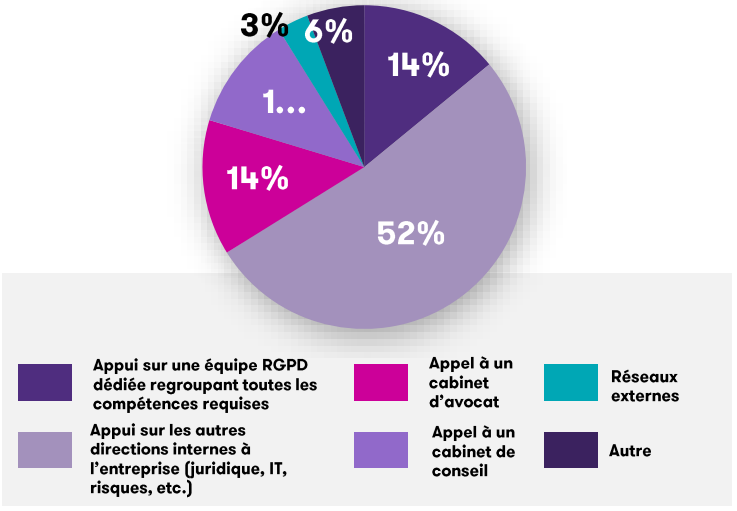
Quant à l'encadrement de proximité, seuls 32 % (cf. annexe graphique N°3) le disent concerné par les enjeux relatifs aux données personnelles. De ce fait, la sensibilisation des collaborateurs est assez faible : 48 % (cf. annexe graphique N°4) affirment que les collaborateurs ne sont pas sensibilisés à la protection des données personnelles dans leurs activités quotidiennes.

Le *DPO* est un chef d'orchestre, dont la direction et les nombreux musiciens sont bien identifiés, mais qui doit encore apprendre à faire jouer ensemble la même partition.

La direction générale est peu accessible et peu à l'écoute des problématiques de protection des données



Comment assurez-vous la pluridisciplinarité nécessaire à la fonction de *DPO* ?



Grant Thornton

Et un réseau d'acteurs à consolider

Le DPO doit devenir un « solution maker » plus qu'un « contrôleur réglementaire ». Pour ce faire, les DPO devront monter en compétence pour couvrir avec une expertise suffisante les volets juridiques, IT et métier de leur entreprise. Une sorte de « DPO by design ».

Me Franklin Brousse
Avocat et Associé fondateur de RGPD Check – plateforme d'évaluation des sous-traitants

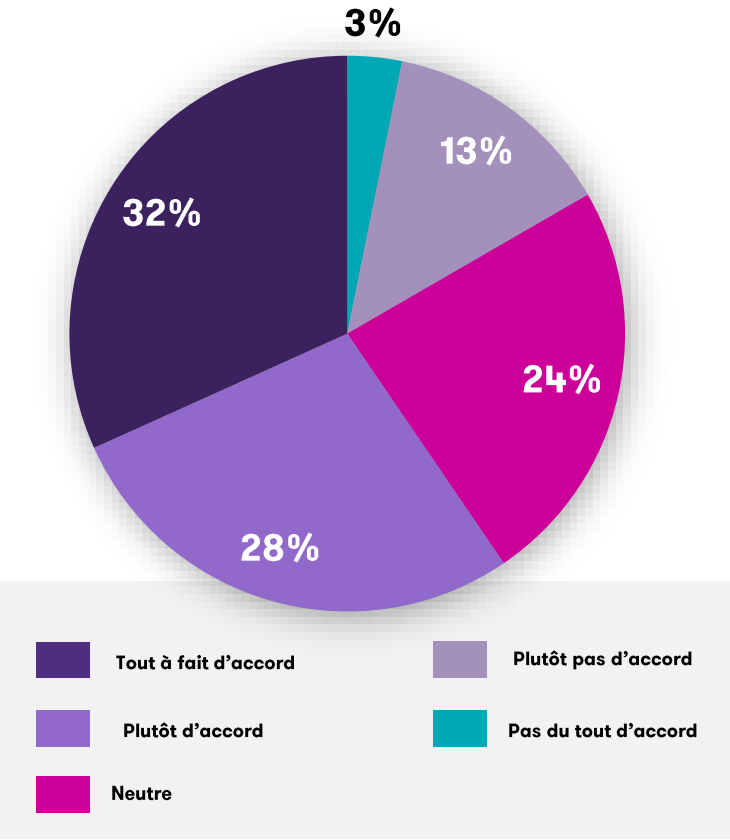
Aujourd'hui, le DPO fait face à un foisonnement législatif et réglementaire hors et intra Europe, lié aussi bien à de nouvelles règlementations relatives à la protection des données que de nouvelles exigences autour de la data (IA Act, data act, EHDS etc.)

Isabelle du Chatelier
Group Data Protection Officer
Dassault Systèmes

Grant Thornton

RGPD : contrainte ou vecteur de croissance ?

Le RGPD est culturellement vu en interne comme une contrainte



Perception culturelle du RGPD

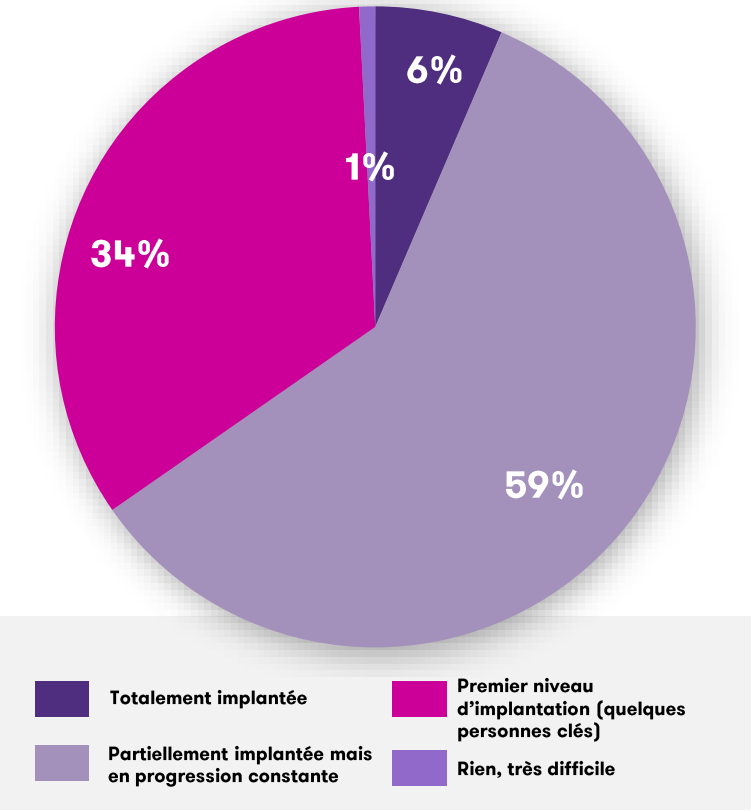
La conformité au RGPD est très largement perçue comme une contrainte pour 60 % des sondés.

Nous mesurons ici l'enjeu pour les *DPO* et les directions générales de **réussir à faire de la conformité RGPD un vecteur de communication interne de sécurité, de confiance** des salariés en leur entreprise, et un vecteur externe de crédibilité de l'organisation à l'égard des tiers.

Grant Thornton

Une implémentation à renforcer

Comment évaluez-vous le niveau d'acculturation à la protection des données ?



Une acculturation au RGPD encore insuffisante

Cette enquête révèle également qu'une large majorité des *DPO* interrogés considère **la conformité RGPD comme partiellement implémentée,** mais toutefois en progression.
Saluons ici le travail des *DPO*, qui parviennent, malgré des moyens très réduits, à faire progresser la conformité.

Toutefois, **les réponses démontrent qu'un nombre élevé d'acteurs ont des difficultés à embarquer les opérationnels sur les sujets de protection des données personnelles et que le niveau d'acculturation reste encore trop faible (34 %).**

Grant Thornton

Nos clés pour une gouvernance adaptée

Une gouvernance efficace en matière de RGPD doit reposer sur :

- Une direction générale accessible et pleinement impliquée dans le projet de déploiement de la conformité au RGPD
- Un positionnement stratégique du *DPO* lui assurant une bonne visibilité au sein de l'organisation, ainsi qu'un rattachement hiérarchique pertinent afin qu'il exerce ses missions en collaboration avec les différents départements internes
- Une sensibilisation de l'ensemble des collaborateurs au RGPD, de la direction, jusqu'au maillage le plus fin de l'organisation
- La mise en œuvre d'audits réguliers afin de déterminer le niveau de maturité en matière de RGPD et les axes de progression envisageables
- L'allocation au *DPO* de moyens humains et matériels nécessaires à la bonne conduite de sa mission

03 Conformité opérationnelle

Grant Thornton

Une conformité RGPD opérationnelle quotidienne

La gestion quotidienne de la conformité opérationnelle au RGPD est un enjeu majeur pour chaque *DPO* s'il souhaite pérenniser son dispositif. La conformité de l'organisation passe par celle des pratiques quotidiennes de chacun de ses membres.

Face à cet enjeu, de nombreux *DPO* ont choisi d'intégrer les principes de protection des données directement dans les processus métiers, par le biais d'un *corpus* documentaire dédié, et par la mise en place de contrôles.

La mise en place de procédures s'est étendue à l'ensemble des strates de l'entreprise avec le RGPD. Ces dernières peuvent être d'ordre général (politique de protection des données), spécifique (gestion des droits) ou métier (gestion des contrats).

Si les procédures RGPD sont aujourd'hui bien implémentées, il reste encore à les faire connaître et à les appliquer.

Afin de s'assurer de la bonne mise en place des principes de protection des données à caractère personnel et de la bonne application des procédures, le *DPO* doit désormais structurer le volet « contrôles permanents » de sa conformité. Ces derniers doivent permettre au *DPO* d'évaluer l'efficience de son dispositif de conformité RGPD. Reste à trouver la bonne formule.

La gestion opérationnelle de la conformité est un exercice hybride pour un *DPO*, alternant entre coopération avec les métiers et « contrôle » de ces derniers.

Grant Thornton

Une conformité opérationnelle déployée...

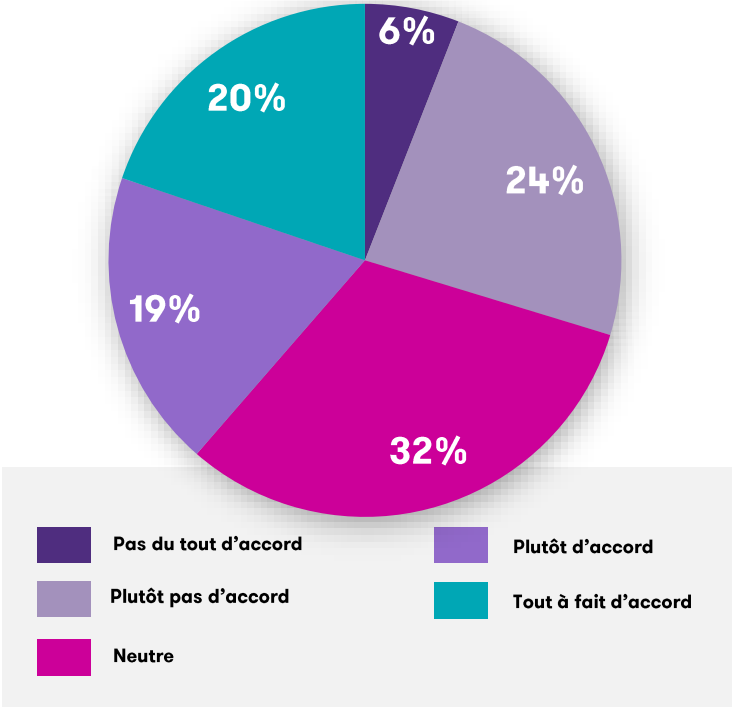
La déclinaison opérationnelle des principes de protection des données passe essentiellement par un **corpus documentaire** et des **outils de conformité** mis en place par le *DPO*.

Afin d'ancrer les bonnes pratiques de gestion des données personnelles au sein des équipes opérationnelles, le *DPO* a une « arme de destruction massive » à sa disposition : **la procédure**. D'ordre général (politique de protection des données, charte de bons usages) ou opérationnel (gestion des violations de données personnelles, gestion des droits des individus, etc.), elles ont été instaurées dans les entreprises ou organismes dès 2018. Aussi, en 2022, 62 % des répondants estiment que **leurs procédures RGPD sont suffisamment déployées et connues des opérationnels**. A cet effet, 65 % des *DPO* ont déclaré être avertis dans les temps d'une demande de droits des individus et 53 % d'une violation de données personnelles ; preuve que ces dernières sont bien connues et maîtrisées en interne par tous. Par ailleurs, **le registre des traitements,** notamment sa **complétude et sa lourdeur, n'est plus un sujet** pour les *DPO* puisque 68 % d'entre eux affirment que celui-ci est en adéquation avec leur entreprise.

Cette situation est notamment due à la mise en place d'outils informatiques gérant tant le registre que les procédures. Ces derniers, soit développés en interne, soit issus d'outils du marché, représentent pour 26 % (cf. annexe graphique N°5) des *DPO* **une aide indispensable** dans la conduite de leur mission.
Toutefois pour plus de la moitié des *DPO* interrogés, **des frustrations subsistent, notamment sur la complexité d'utilisation** (paramétrage, gestion) **et le coût de revient annuel** qui reste élevé (licence et ressources pour l'administrer).

Ainsi, les outils à la main du *DPO* permettraient de garantir une déclinaison opérationnelle efficiente des obligations issues du Règlement Général sur la Protection des Données.

Mes procédures ne sont pas à jour ou insuffisamment connues et déployées



« La mise en place de notre outil de conformité nous a permis de déployer, sur l'ensemble du périmètre, la « Privacy by design »

Sarah Taïeb-Jaskierowicz
***Global DPO* UGI**

Grant Thornton

… avec des modalités de contrôle non définies

Malgré de nombreux outils existants et déployés, **le contrôle du correct déploiement des mesures de gestion et de traitement des données personnelles reste un point d'amélioration pour le *DPO*.**

La conformité au RGPD étant très opérationnelle, **seules la conscience et l'application quotidiennes de pratiques conformes par les collaborateurs, en garantiront le respect.**

Force est de constater **qu'il n'existe pas d'uniformité dans les processus de contrôle de conformité** réalisés par les *DPO*. En effet, 26 % déclarent réaliser des **contrôles ponctuels** ciblés et réguliers, contre 42 % optant pour un **audit de conformité annuel unique** réalisé soit par les équipes internes (*DPO*, audit ou contrôle interne) soit par un cabinet externe (avocat, cabinet de conseil, etc.). Enfin, 15 % ne réalisent pas de contrôle de conformité.

Malgré cela, aucun *DPO* n'a déclaré qu'un contrôle de conformité n'était pas nécessaire.

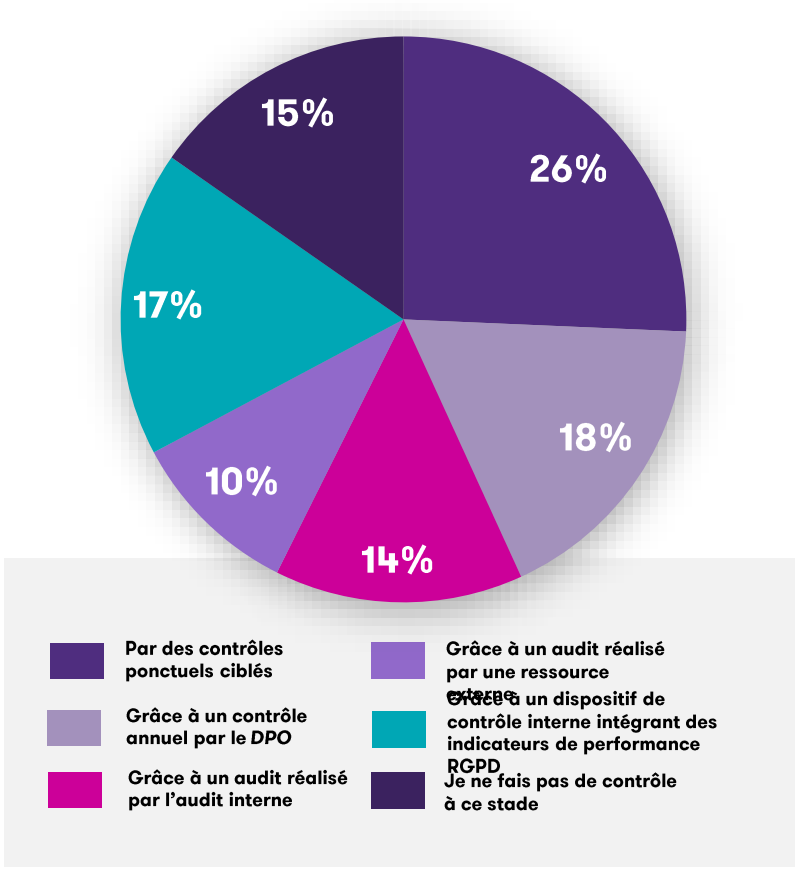
Notons que déjà 17 % des répondants lient leurs contrôles RGPD à leurs dispositifs de maîtrise des risques.

Ce résultat est sans doute la conséquence du rattachement - en augmentation - des *DPO* aux fonctions de gestion des risques dans l'entreprise.

Face à la multitude de modalités de contrôles et de pratiques, on peut s'interroger sur la pérennisation des dispositifs de conformité RGPD au sein des processus métiers et plus largement des dispositifs de maîtrise des risques des entreprises en 2022.

Le rattachement observé du *DPO* à des fonctions de risques est peut-être lié à une prise de conscience de cette situation et un début de réponse.
Force est de constater que la conformité au RGPD s'intègre assez naturellement au sein du dispositif global de contrôle interne et de maîtrise des risques opérationnels.

Comment vous assurez-vous de la conformité RGPD de votre organisation ?



Grant Thornton

Nos clés pour une conformité opérationnelle

Pour mettre en place une conformité opérationnelle adéquate, le *DPO* doit appliquer les grands principes suivants :

- Adapter les procédures RGPD à l'environnement métier et général de l'entreprise
- Outiller informatiquement la fonction afin d'éviter la multitude de documents
- Définir un plan de contrôle ponctuel et annuel, intégré au contrôle interne de l'entreprise

04 Gestion des tiers et gage de conformité

Grant Thornton

Le « casse-tête » de la gestion des tiers

La gestion de la relation avec les tiers, pendant ou après la contractualisation, reste un « casse-tête » pour les *DPO*.

Alors que les relations avec un sous-traitant doivent être encadrées par un dispositif contractuel comprenant certaines clauses obligatoires (article 28 RGPD), 58 % (cf. annexe graphique N°6) **des *DPO* ne sont pas certains que cela soit le cas au sein de leur organisation.**

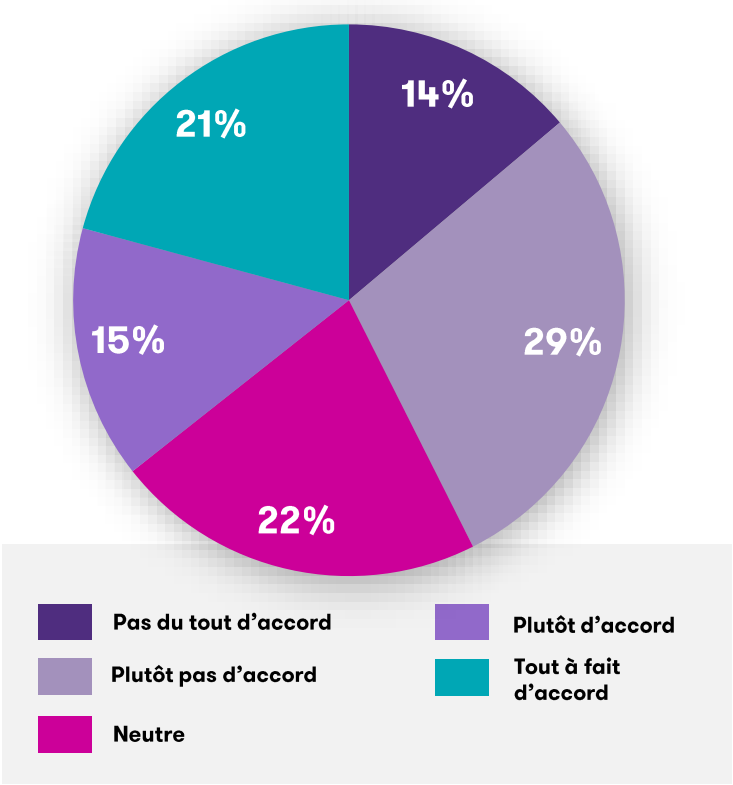
Les difficultés ne s'arrêtent pas au seul sujet contractuel. Le responsable de traitement doit s'assurer que celui-ci respecte ses obligations légales et contractuelles. Ce travail de vérification reste encore trop lourd et complexe à gérer pour les *DPO*, notamment lorsqu'ils ne sont pas rattachés à la fonction juridique.

En matière de contrôle des tiers, les *DPO* sont encore à la recherche du meilleur processus car ils sont peu satisfaits des méthodes existantes, notamment l'envoi de questionnaires de conformité qui s'avère extrêmement pénible à traiter et chronophage.

Grant Thornton

Un flou contractuel

Je n'ai pas l'assurance que nos contrats intègrent toutes les exigences du RGPD



L'entrée en vigueur du Règlement Général sur la Protection des Données a entraîné des évolutions majeures en termes de contractualisation et de processus de validation des contrats. Ce règlement a également eu la vertu de conduire à un recensement des contrats au sein des entreprises.

En 2022, le cauchemar contractuel demeure, et la gestion des contrats pour un *DPO* reste encore l'un des volets les plus lourds à traiter en matière de conformité RGPD.

Les difficultés qu'ils rencontrent dans ce domaine sont de deux ordres :

- **L'identification de l'ensemble des contrats** signés par son organisation,
- **Le contrôle** que ceux-ci comportent l'ensemble des clauses obligatoires et **les réviser** le cas échéant.

Sur ce dernier point, 36 % estiment **ne pas avoir l'assurance que leurs contrats sont conformes aux exigences du RGPD** et ce, malgré le fait que leur fonction soit devenue incontournable dans le cadre de ce processus.

Cette situation est la conséquence de ***DPO* pas ou peu sollicités dans le processus de contractualisation,** mais également de pratiques internes persistant au sein des équipes opérationnelles.

Il ressort que le profil de *DPO* adapté pouvant faire face à ces difficultés aura des compétences juridiques suffisantes ou un positionnement lui permettant d'y accéder (rattachement au juridique), et des outils adaptés (librairie de contrats notamment). Le *DPO* disposant d'un réseau interne (correspondants métiers et fonctions supports) aura de ce fait plus de visibilité sur les nouveaux contrats.

Pour ces raisons, les obligations en termes de contractualisation définies dans le RGPD ont du mal à être appliquées.

Le recensement des contrats, induit par le RGPD aura permis aux directions juridiques de remettre à plat le processus de contractualisation.

Grant Thornton

Un contrôle de la conformité des tiers qui cherche son modèle

Face à l'obligation de s'assurer que les partenaires des entreprises soient en conformité avec le RGPD, tout *DPO* se questionne légitimement sur la bonne manière de faire.

Si les questionnaires de conformité restent l'outil principal de gestion de la conformité RGPD des tiers, 43 % des répondants estiment que ces derniers sont lourds à gérer quotidiennement.

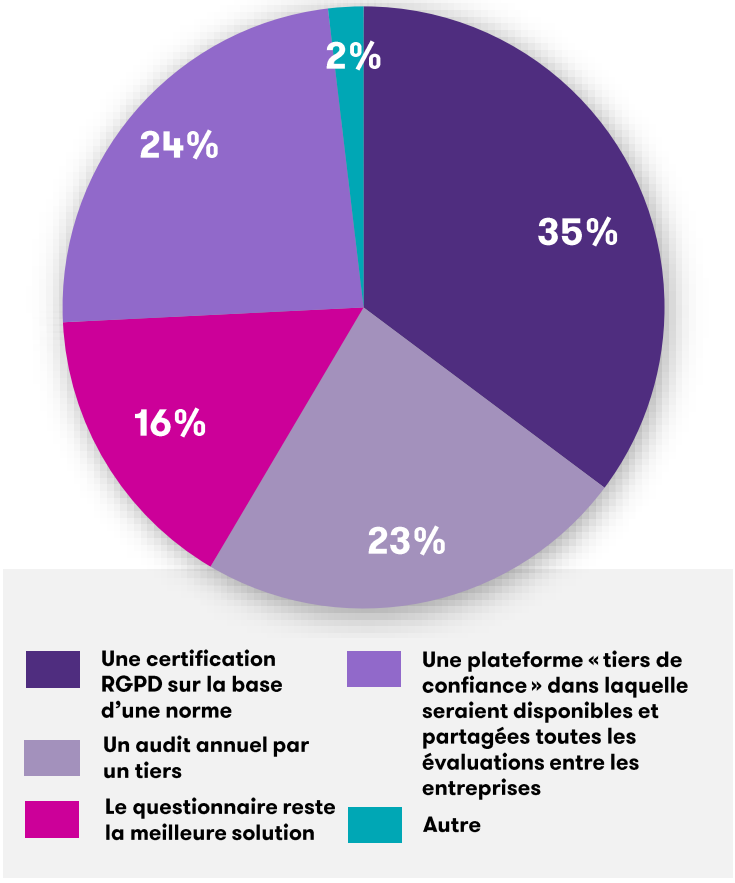
Pour y remédier, les *DPO* plébiscitent les solutions externes, portées par le marché, les autorités ou la CNIL, comme une alternative viable. Plusieurs options sont évoquées : 35 % souhaitent **qu'une certification RGPD** se mette en place, 23 % prônent un **audit annuel par un tiers externe** (cabinet d'audit) et 24 % des solutions du **type plateforme « tiers de confiance »**.

Pour ce qui est de **la certification de conformité** telle que prévue par l'article 57(1)(n) du RGPD, elle **se met enfin en place.** *Europrivacy* a été validé par le CEPD (Comité Européen de la Protection des Données) comme Label européen de protection des données pour évaluer et certifier la conformité de toutes sortes de traitements de données avec le RGPD.

Toutefois, les *DPO* restent à la recherche de solutions externalisées pour les aider dans cette tâche.

Concernant les gages de conformité des tiers, le chantier reste ouvert. Les solutions actuelles, même digitales (envoi de questionnaires) sont trop chronophages et sans réelle valeur ajoutée. La solution des plateformes « tiers de confiance » est séduisante car elle permet de digitaliser l'évaluation, et donne au sous-traitant la possibilité de la partager avec ses responsables de traitement. Une nouvelle solution se met en place avec la certification Europrivacy.

Quelle serait, selon vous, la bonne alternative à l'utilisation des questionnaires de gages de conformité pour les tiers ?



Grant Thornton

Nos clés pour la gestion des tiers

Le contrôle de la relation avec les tiers passe par les éléments suivants :

- Intégrer le *DPO* au processus de contractualisation pour lui donner de la visibilité et lui permettre d'émettre des avis
- Prioriser les actions en s'intéressant en premier aux contrats à fort enjeu ou portant un risque important
- Outiller les équipes en charge de contractualiser et de gérer la relation avec les tiers : clauses types, questionnaires, grille d'évaluation des risques, etc.
- La certification et les plateformes tiers de confiance sont une alternative pertinente
- Maintenir à jour un registre des contrats détaillant l'état des clauses RGPD et les gages fournis par les sous-traitants

05 Sécurité des données

Grant Thornton

La sécurité des données : entre exigences et réalité opérationnelle

La sécurité des données s'inscrit pleinement dans le processus de mise en conformité au RGPD. Cette exigence, formulée par l'article 32 du règlement, est en filigrane de tous les autres sujets de conformité au RGPD et requiert des compétences diverses que le *DPO* se doit de mettre en œuvre.

Ce sujet de la sécurité n'a pas attendu le RGPD pour exister. Il était déjà l'une des principales missions des DSI et RSSI. Aussi, le *DPO* doit à la fois s'insérer dans le dispositif existant des DSI, mais aussi le faire évoluer sur des sujets spécifiques à la protection des données.

Ainsi, les *DPO* n'étant pas nécessairement spécialisés en gestion des systèmes d'information et en sécurité informatique, doivent souvent coopérer avec leur DSI ou avec des prestataires informatiques, selon la taille et le type de leur structure. C'est le cas lors de la conduite de PIA (*Privacy Impact Assessment*) dans un cadre préventif mais aussi en cas de violation de données.

La sécurité dépend de bonnes pratiques quotidiennes et des réflexes que les collaborateurs doivent acquérir. Or ces nouvelles habitudes de fonctionnement sont souvent mal perçues, comme venant perturber les processus existants.

La sécurité exige un niveau de sensibilisation suffisant des collaborateurs pour être correctement prise en compte, elle doit devenir un réflexe et être complètement intégrée aux pratiques.

Grant Thornton

La sécurité des données ne se limite pas aux systèmes d'information

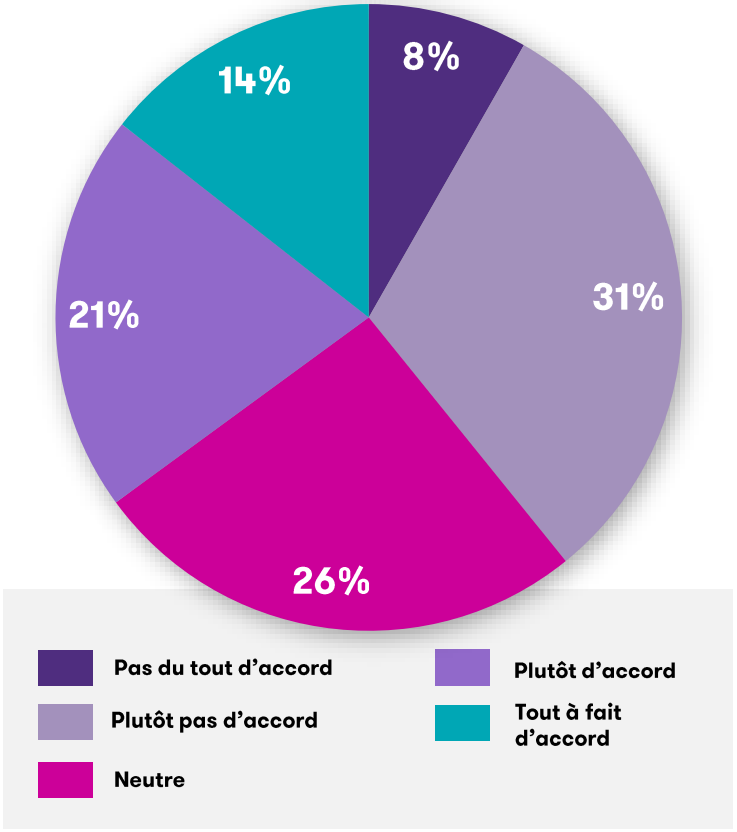
La direction des systèmes d'information a un rôle essentiel dans la gestion de la sécurité des données à caractère personnel et dans la maîtrise des processus inhérents à leurs traitements. D'ailleurs, 60 % (cf. annexe graphique N°7) des répondants estiment que **les exigences du RGPD en matière de sécurité des données sont suffisamment prises en compte** par les équipes de la DSI de leurs structures.

Mais toutes les données personnelles ne se trouvent pas seulement dans les systèmes d'information, et leur sécurité dépend également des pratiques quotidiennes des collaborateurs. Or les convaincre et faire évoluer leurs pratiques, nécessite de la part du *DPO* de la constance dans la formation et la sensibilisation.

La sécurité est parfois perçue comme antinomique avec la performance des activités. En effet, la question : « **la sécurité est-elle un frein à l'activité ?** », divise notre panel : 35 % sont d'accord avec cette affirmation, 39 % ne le sont pas et 26 % se positionnent entre les deux.

Cette ambivalence révèle que **la sécurité des données hors système d'information comporte des marges de progrès ;** et ce volet du RGPD reste donc une thématique perçue comme globalement contraignante pour les équipes opérationnelles.

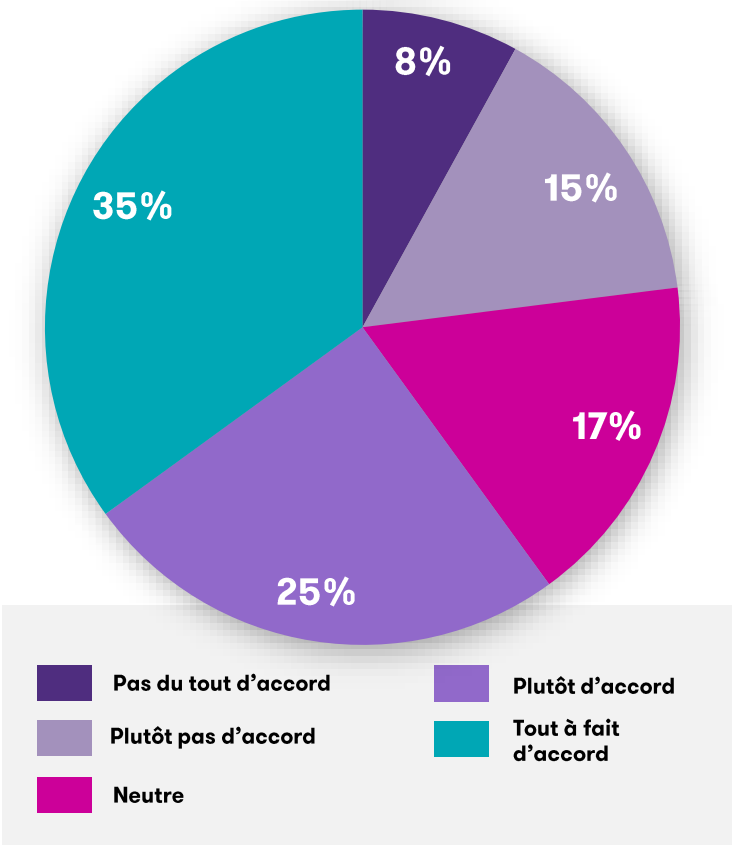
Les collaborateurs pensent que la sécurité, bien que nécessaire, est un frein à leur activité



Grant Thornton

Les analyses d'impact : un exercice difficile

Les analyses d'impact sur la vie privée sont difficiles à mener



Face aux exigences de sécurité des données, le *DPO* peut s'appuyer sur deux dispositifs qui accompagnent ses actions et ses diligences :

- en amont, les analyses d'impacts,
- en aval, la gestion des violations de données personnelles.

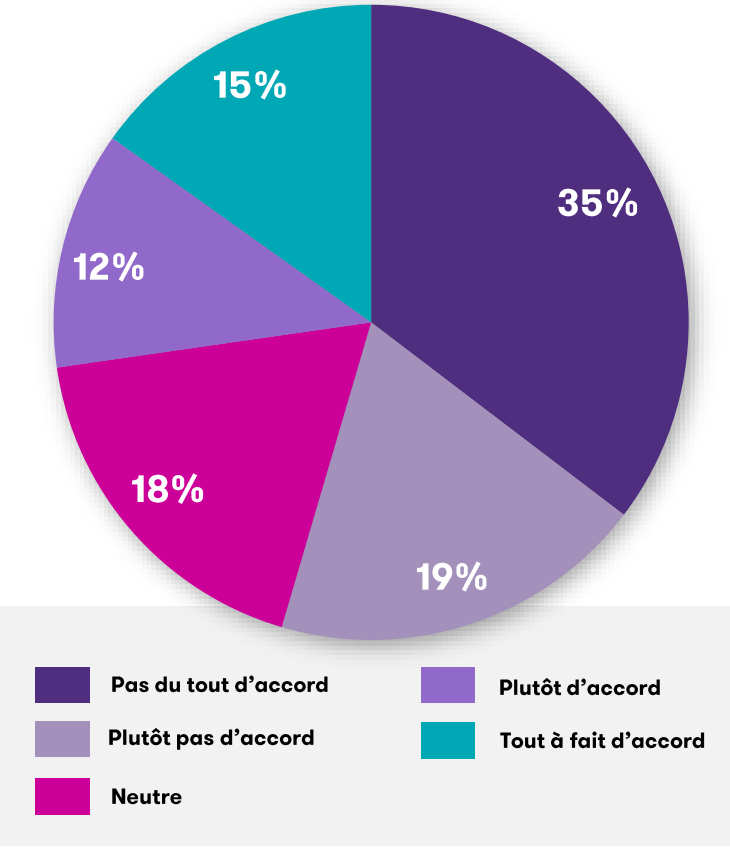
Les analyses d'impact constituent un premier niveau de sécurité des données car elles soulignent les failles éventuelles d'un traitement dit à risques, selon les conditions prévues par l'article 35 du RGPD.

Bien qu'indispensable aussi bien au regard de la conformité au RGPD que des bonnes pratiques de sécurité, **la conduite de ces analyses demeure une problématique** pour une majorité des répondants. En effet, 60 % des sondés les considèrent comme difficiles à mener.

Cette difficulté s'explique notamment par le manque d'implication des directions concernées et la lourdeur de l'analyse à mener.

Une bonne organisation du processus de traitement des violations de données

Je suis informé(e) trop tardivement ou non exhaustivement des situations de violation de données



Si la correction d'une faille de sécurité peut parfois constituer un casse-tête pour les organismes qui en sont victimes, **leur détection et la circulation de l'information semblent bien être prises en compte.**

En effet, le traitement des failles de sécurité, en bout de chaîne de la sécurité des données, est **jugé adéquat et exhaustif** par 54 % des *DPO* interrogés.

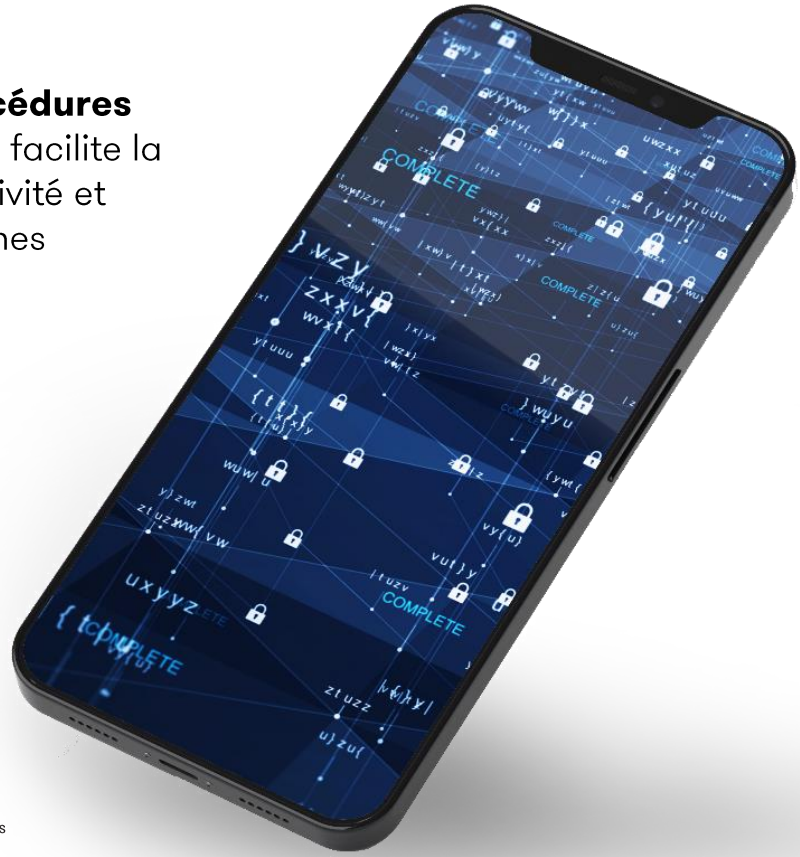
Cette tendance se confirme avec la confiance que placent les *DPO* interrogés dans leur DSI, qui joue un rôle majeur dans le traitement de ces failles.

Nos clés pour la sécurité des données

Pour mettre en place une sécurité des données adéquate, le *DPO* doit appliquer les grands principes suivants :

S'appuyer sur l'existant. Il existe des outils prévus pour conduire des analyses d'impact ou pour gérer des violations de données

Rédiger des procédures de sécurité. Cela facilite la continuité de l'activité et pérennise les bonnes pratiques



Coopérer avec les directions expertes. La DSI est perçue comme l'acteur le plus à même de résoudre les problématiques relatives à la sécurité des données

Définir des contrôles applicatifs au sein des outils gérant et stockant des données à caractère personnel. Ces contrôles déchargent les collaborateurs qui peuvent se focaliser sur leur tâches

06 Conclusion

Grant Thornton

Quel avenir pour le *DPO* ?

Après plusieurs années passées sur des programmes de mise en conformité RGPD qui arrivent à leur terme, la fonction de *DPO* est entrée dans une phase de mutation. Quelques lignes directrices se dessinent, sans pour autant être définitives. Parmi elles, trois nous semblent particulièrement intéressantes :

Dans un premier temps, une dimension de plus en plus grande de la notion de « risque » dans la fonction du *DPO*.

Cela se traduit selon différentes formes :

- Un rattachement aux fonctions risques de l'entreprise : contrôle interne, contrôles permanents, gestion des risques, etc.
- Une approche de la conformité par les risques, pour arbitrer les moyens mis à disposition du *DPO* et répondre à la question : quel est le risque de ma non-conformité et comment adapter mon plan d'actions en fonction de ce niveau de risque ?

Dans un second temps, un élargissement du périmètre couvert par le *DPO*. Ce dernier verrait son champ d'intervention s'élargir à l'ensemble des données, non plus seulement aux données personnelles. Cette évolution permettrait ainsi une meilleure cohérence avec l'évolution réglementaire qui foisonne autour de la *data* et avec l'organisation interne des entreprises.

Enfin, la fonction de *DPO* glisse de plus en plus de la conformité pure vers de la gestion de projet interne (*privacy by design notamment*), du contrôle de conformité, sachant que, dans le même temps, les aspects liés à la conformité deviennent de plus en plus techniques, dans les domaines IT et juridique entre autres.

Grant Thornton

Quel avenir pour le *DPO* ?

La vision de la conformité passe par une vision intégrée des risques vers laquelle doit aller le DPO.

Olivier Guillo
Founding partner
Smart Global Governance

L'imbrication des données personnelles et des données non personnelles implique nécessairement l'évolution du métier de DPO vers une fonction plus globale de Data Regulation Officer ou de Data Ethic Officer.

Aurélie Banck
DPO, Compliance Officer
Europcar Mobility Group

Plus qu'un chef d'orchestre de la conformité, le DPO devient un facilitateur entre les fonctions métiers pour l'amélioration des processus internes et un ambassadeur de la culture et des valeurs de l'entreprise.

Jennifer Godin
***DPO* du groupe ROQUETTE**

Une réflexion sur le positionnement du DPO comme acteur de la conformité au sens large au sein de l'entreprise, doit se poser à l'avenir.

Michel Seigne
DPD Touraine Logement

L'intégration des données personnelles dans une gouvernance plus large de la donnée va amener sans doute les entreprises à créer un rôle de Data Officer qui va bien au-delà de celui du DPO.

Isabelle du Chatelier
Group *Data Protection Officer*
Dassault Systèmes

Grant Thornton

Conclusion

Les résultats de cette enquête montrent le chemin parcouru par les *DPO* depuis la date d'entrée en vigueur du RGPD.
Il convient de saluer leur travail, leur implication et leur ténacité à implémenter cette règlementation dans leurs organisations.

Même si en matière de conformité cette dernière n'est jamais acquise, cette enquête montre que certains chantiers restent à initier. Parmi ceux à traiter se trouvent la gestion des contrats et les gages de conformité des tiers, mais aussi la sensibilisation des collaborateurs à ce jour insuffisante, ou encore, spécifiquement pour les groupes, la gestion multiréglementaire des législations locales en matière de protection des données personnelles.

Il est aussi particulièrement intéressant de noter avec le temps, les évolutions qui se dessinent et notamment la dimension de plus en plus grande de la gestion des risques, d'approche par les risques, que prend cette fonction.

En effet, c'est bien par les risques que cette conformité doit être appréhendée, implémentée et contrôlée. En amont, afin de bien discerner les enjeux de conformité qui sont radicalement différents d'une organisation à une autre selon qu'elle opère en *Business to Business* ou en *Business to Consumer*, ou selon la quantité, la sensibilité, ou encore la complexité de données qui est gérée, stockée, utilisée.
Et en aval, afin d'assurer une conformité dans le temps.

Les dispositifs socles mis en place par les *DPO* ne sont ni plus ni moins qu'un dispositif de contrôle interne centrés sur les données personnelles.
L'enjeu, maintenant, va être de faire en sorte que ce dispositif de contrôle interne intègre les processus de contrôle de l'entreprise, lui assurant un *monitoring* et une dynamique d'amélioration continue, que l'audit interne pourra contrôler au gré de ses plans d'audit.
Les *DPO*, chefs d'orchestre de cette conformité, n'ont pas fini de faire évoluer leur métier !

Nicolas Gasnier-Duparc
Associé *Business Risk Services*,
En charge de l'offre *Data Privacy*
Grant Thornton

Nicolas Rémy-Néris
Avocat
DPO externalisé
Grant Thornton Société d'Avocats

Avec les contributions de

Simon Evain
Manager RGPD

Arnaud Humbert
Consultant *senior* RGPD

Mathias Grinbaum
Consultant *senior* RGPD

Pauline Garcia
Avocate en protection des données

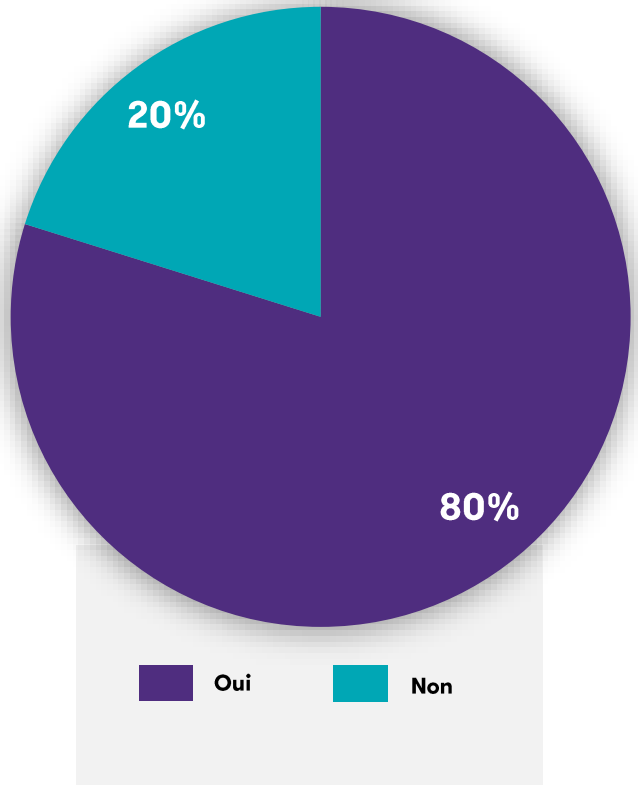
Grant Thornton

Annexes

Annexe

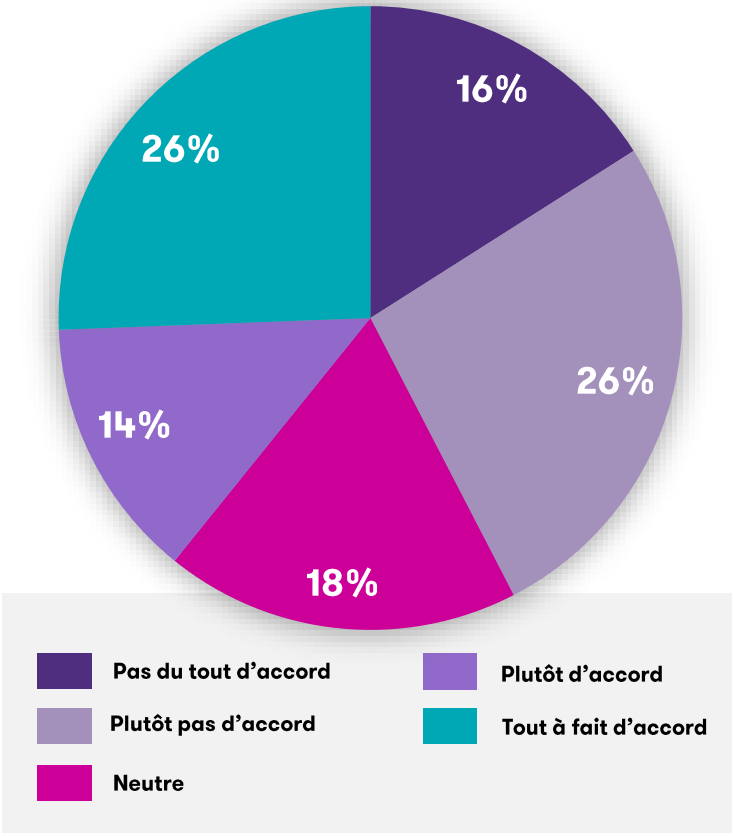
Graphique N°1

Ce rattachement est-il pertinent selon vous ?



Graphique N°2

Le positionnement du DPO dans l'organisation ne lui donne pas la visibilité nécessaire

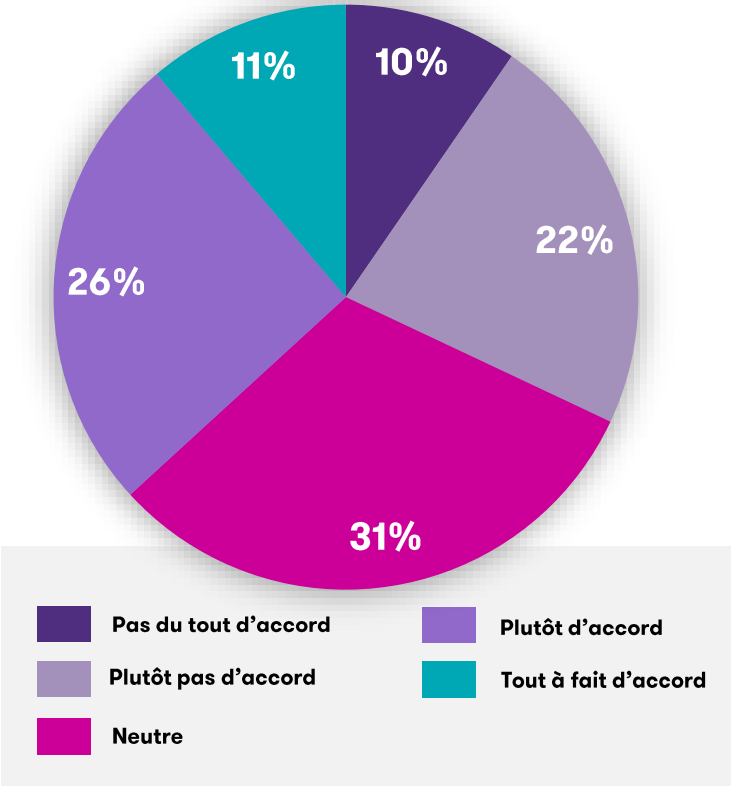


Grant Thornton

Annexe

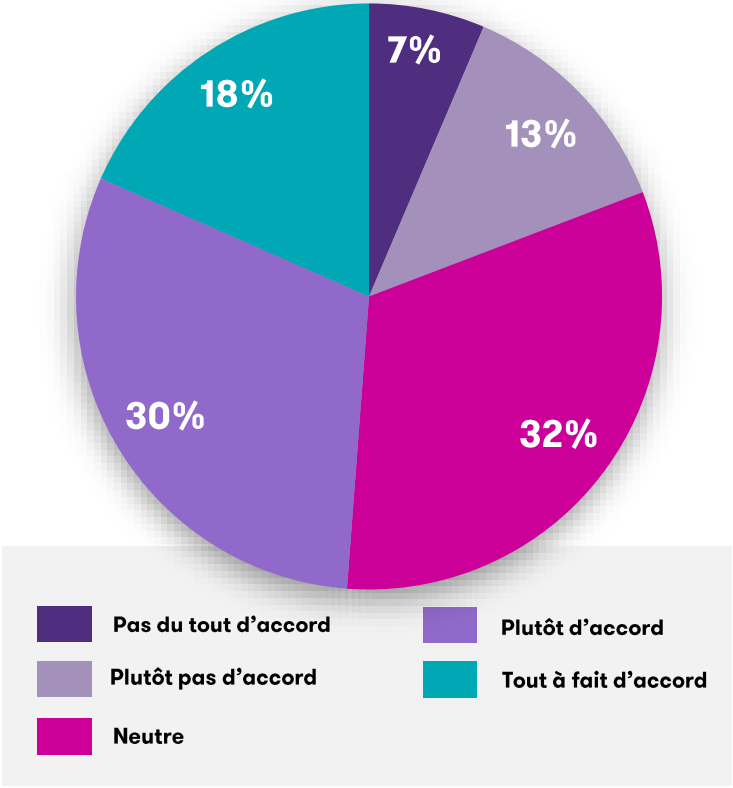
Graphique N°3

L'encadrement de proximité ne se sent pas concerné par le RGPD



Graphique N°4

Les collaborateurs, dans leurs tâches quotidiennes, ne sont pas suffisamment sensibilisés aux exigences du RGPD

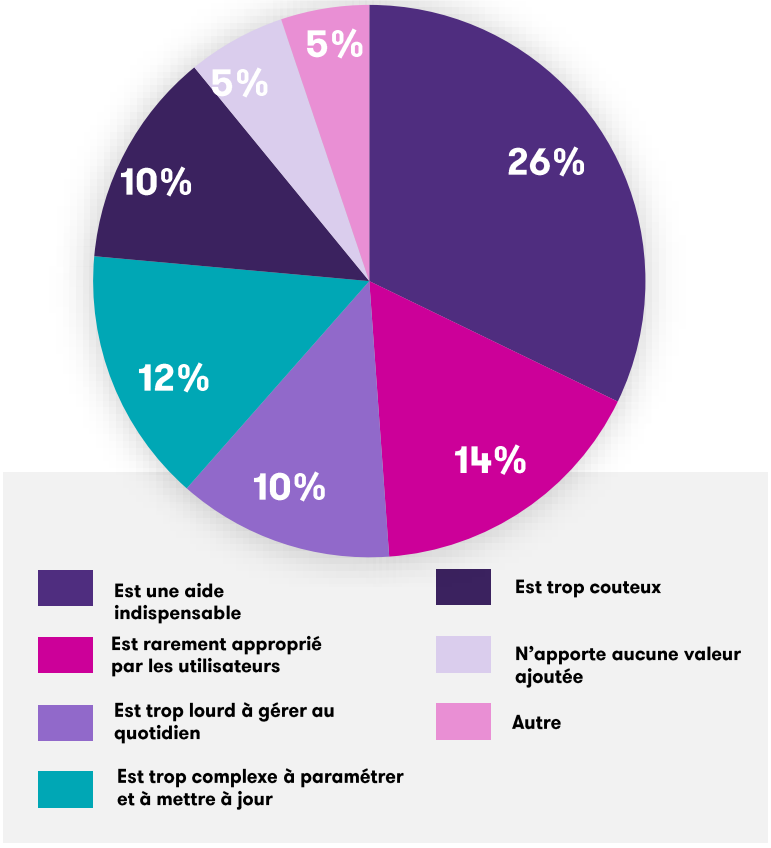


Grant Thornton

Annexe

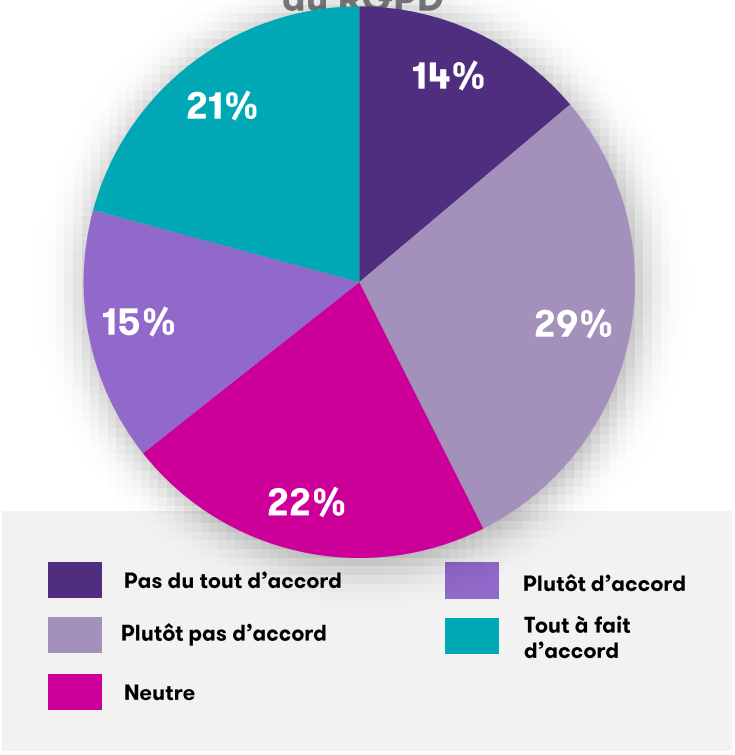
Graphique N°5

Selon vous, un outil informatique de gestion de la conformité RGPD



Graphique N°6

Je n'ai pas l'assurance que nos contrats intègrent toutes les exigences du RGPD

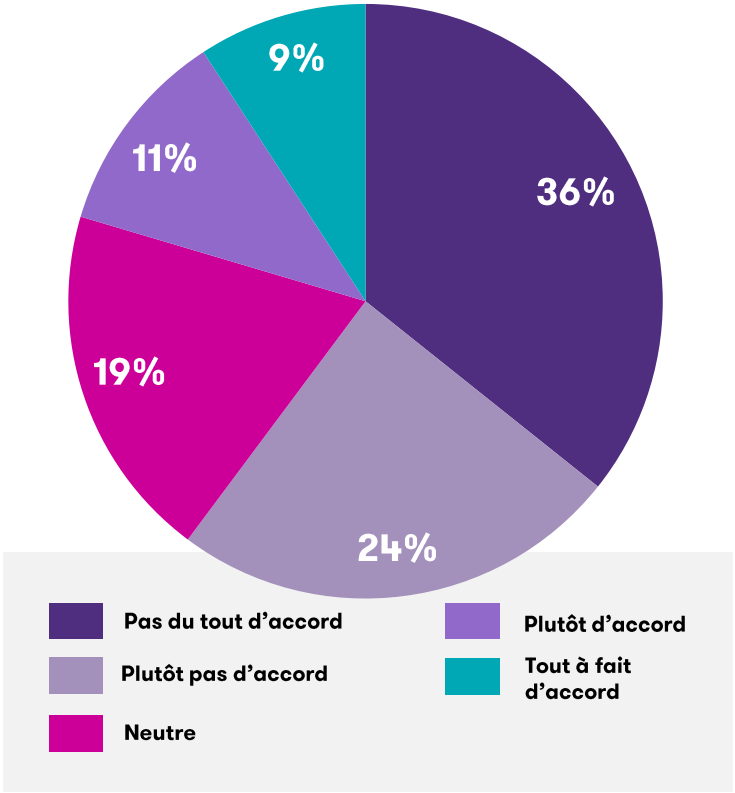


Grant Thornton

Annexe

Graphique N°7

Les exigences du RGPD en matière de sécurité numérique des données ne sont pas assez prises en compte par la DSI



Grant Thornton

Grant Thornton

grantthornton.fr

Grant Thornton
Société d'Avocats

avocats-gt.com

Agnès de RIBET
Associée,
en charge du *Marketing*,
de la Communication
et du *Business Development*
T + 33 (0)1 41 25 85 85
E agnes.deribet@fr.gt.com

Grant Thornton