LE GUIDE DU DPO PRÊT À L'ACTION !

Le DPO, garant du RGPD
Incarner la fonction de DPO
Les outils et le quotidien du DPO

www.everteam.com

everteam
A KYOCERA GROUP COMPANY

Sommaire

Introduction

Le DPO, pour Data Protection Officer — également appelé DPD, Délégué à la protection des données — se trouve au centre du tant attendu Règlement général sur la protection des données.

Applicable à partir du 25 mai 2018 dans tous les pays membres de l'Union européenne, adopté par la Commission européenne en avril 2016, le RGPD (GDPR en anglais) a une ambition : redonner aux citoyens le contrôle sur leurs données, telles qu'elles sont exploitées, utilisées et communiquées par les entreprises qui les ont récupérées.

Issu de longues années de négociation entre les acteurs économiques et les législateurs, comptant quelque 99 articles et 173 considérants, il doit aider l'Europe et les entreprises à s'adapter aux nouvelles réalités du numérique.

Il repose notamment sur un consentement explicite et positif des personnes concernées (qu'il s'agisse de particuliers ou de professionnels) dont les informations sont récupérées, sur un droit à l'effacement et à la portabilité (et sur la possibilité pour chacun d'accéder à ce droit, en moins d'un mois), ainsi que sur un cadre (enfin !) harmonisé au niveau européen.

Il impose donc aux acteurs économiques de répondre à de nouvelles exigences. Un carcan ? Pas vraiment : il est aussi possible de voir le RGPD comme une mesure à même de renforcer la confiance accordée aux marques et aux acteurs économiques !

Le RGPD constitue donc un impératif, un document de référence, pour toute entreprise soucieuse de l'utilisation des données dans ses process. Pour cela, 6 étapes de mise en conformité ont été identifiées par la CNIL, organisme qui a pour charge, en France, de vérifier que le Règlement est bien appliqué par les acteurs économiques :

- La désignation d'un pilote ;
- La cartographie du traitement des données personnelles ;
- La priorisation des actions correctrices à apporter sur le traitement de ces données ;
- La gestion des risques ;
- La réorganisation des processus internes ;
- La documentation des ajustements opérés.

Là où intervient le DPO ? Un peu partout, et ce dès la première des étapes identifiées par la CNIL ! Il doit en effet être le pilote de l'application du RGPD en entreprise. Il en est le référent. Celui qui priorise, décide, améliore le traitement des données. Il a donc un rôle incontournable, transversal, unique.

C'est là tout l'objet de ce Livre blanc, que nous avons intitulé "Le guide du DPO prêt à l'action". "Prêt à l'action", parce que nous avons pour ambition de proposer un document de référence, qui aidera ceux qui sont amenés à devenir DPO à comprendre leur rôle et les outils qui peuvent être à leur disposition.

"Prêt à l'action", parce que ce poste nouveau, cette responsabilité inédite, peut avoir des conséquences non-négligeables pour les entreprises — on parle d'ores et déjà d'amendes s'élevant à plusieurs centaines de milliers d'euros ! — et qu'il convient, donc, d'être irréprochable dans sa pratique quotidienne, dès le 25 mai 2018, date de l'entrée en vigueur du RGPD.

everteam
A KYOCERA GROUP COMPANY

LE DPO, GARANT DU RGPD

Un DPO, pour qui ?
CIL et DPO, ce n'est pas (vraiment) la même chose !
DPO : quelles qualités, quelles compétences ?
La mission du DPO : le respect du RGPD

www.everteam.com

everteam
A KYOCERA GROUP COMPANY

Le DPO, garant du RGPD

Un DPO, pour qui ?

La fonction de DPO a été encadrée, mais aussi créée, par la Commission européenne lorsqu'elle a voté le RGPD. Ainsi, la présence dans l'entreprise d'un Data Protection Officer est obligatoire dans certains cas. Lesquels ? Réponse tout de suite !

Le DPO, obligatoire dès lors qu'un certain volume de données est traité

Chargé de mettre en œuvre la conformité au Règlement européen sur la protection des données (RGPD) au sein de l'organisme qui l'a désigné, le DPO constitue un nouveau profil dans l'entreprise, pas si éloigné que ça du CIL — mais aussi très différent de lui, nous en reparlerons. Sa désignation est obligatoire pour :

- Les autorités ou les organismes publics (les administrations, les ministères…) ;
- Les organismes dont les activités imposent de réaliser un suivi "régulier et systématique", à grande échelle, des personnes (ici, on parle bien sûr des entreprises) ;
- Les organismes dont les activités de base les amènent à traiter à grande échelle des données considérées comme sensibles (les données génétiques, biométriques, afférentes à la santé, à la religion, aux opinions politiques ou à l'appartenance syndicale…) ou en lien avec des condamnations pénales et/ou des infractions.

Obligatoire, mais aussi fortement recommandé !

L'Union européenne aurait pu décider que le DPO était obligatoire "à partir de X salariés dans l'entreprise", "dès lors que des données sont exploitées", ou encore "à partir de X millions de chiffre d'affaires". Elle n'en a rien fait, et pour plusieurs raisons. D'une part, de tels seuils n'auraient pas placé le traitement des données — et le fait qu'elles soient collectées — au cœur des préoccupations. Ensuite, cela aurait forcément créé des inégalités. Enfin, les entreprises situées en dessous de ces seuils classiques auraient pu échapper à la nomination d'un DPO... alors que cela ne les empêche pas de mettre en oeuvre le RGPD !

Reste que les critères pour la désignation d'un DPO sont assez vagues et sujets à interprétation. Où commence, par exemple, le suivi "régulier et systématique" ? À partir de quel volume de données estime-t-on que l'on se trouve face à un traitement "à grande échelle" des données ? Les réponses à ces questions ont été apportées en avril 2017 :

- Un suivi régulier est un suivi continu ou ponctuel, récurrent ou itératif, en cours ou se produisant pendant des périodes données ;

- Un suivi systématique est un suivi prévu, organisé ou méthodique, causé par un système, ou intégré à un plan général de récupération de données ou à une stratégie globale.

- Quant à la "grande échelle"... elle dépendra du nombre de personnes concernées, du volume des données, de la durée de l'activité de traitement et de son périmètre géographique.

C'est pourquoi, en dehors des cas de désignation obligatoire et évident, la désignation d'un responsable de la protection des données est fortement encouragée par les membres de l'Union européenne. Même s'il n'a pas le titre de DPO, il devra être en mesure d'identifier et de coordonner les actions à mener en matière de protection des données personnelles.

DPO interne ou externe ?

Reste une question : le DPO doit-il impérativement être interne à l'entreprise ? Sur ce point, le RGPD est très clair. Le Délégué à la protection des données peut être interne, comme externe. Il peut même être mutualisé au sein d'un groupe d'entreprises, à plusieurs conditions :

- Chacune doit pouvoir lui offrir les conditions propices à l'exercice de ses nouvelles responsabilités ;

- Il ne doit pas y avoir de conflit d'intérêts ;

- Il doit être joignable facilement à partir de chaque lieu d'établissement.

Vous êtes dans l'un des cas où le DPO est obligatoire ? Ne voyez pas cela comme une contrainte mais, au contraire, comme une chance d'optimiser vos process et le traitement de vos données !

everteam
A KYOCERA GROUP COMPANY

Le DPO, garant du RGPD

CIL et DPO, ce n'est pas (vraiment) la même chose !

Le Correspondant Informatique et Libertés, référent sur les questions de protection des données personnelles au sein de l'organisme qui l'a désigné, semble être l'équivalent du DPO. Or, le second serait plutôt le successeur naturel du premier. Explications.

CIL, qui es-tu ?

Chargé des questions liées à la protection des données, le CIL (Correspondant informatique et libertés) a plusieurs missions :

- Garantir la conformité de son entreprise à la loi Informatique et Libertés ;
- Veiller à la sécurité des données utilisées par son employeur ;
- Centraliser les traitements des données…

De telles responsabilités rappellent forcément celles qui incomberont, à partir de du 25 mai 2018, au DPO. Les deux fonctions ne sont cependant pas exactement les mêmes.

Plus d'exigences…

Le Règlement général sur la protection des données précise en effet que de nouvelles exigences s'imposent au DPO s'agissant de ses qualifications et de ses connaissances.

Il doit notamment — nous y reviendrons — posséder certains savoirs en matière de droit et de pratiques. Et il doit veiller à entretenir ces connaissances spécifiques, via un programme de formation continue.

Autant d'impératifs qui ne concernaient pas vraiment le CIL, dont le rôle se limitait finalement à rassurer les clients de l'entreprise, les fournisseurs, les partenaires potentiels, le personnel… et les autorités de contrôle, la CNIL en premier lieu !

everteam
A KYOCERA GROUP COMPANY

Le DPO, garant du RGPD

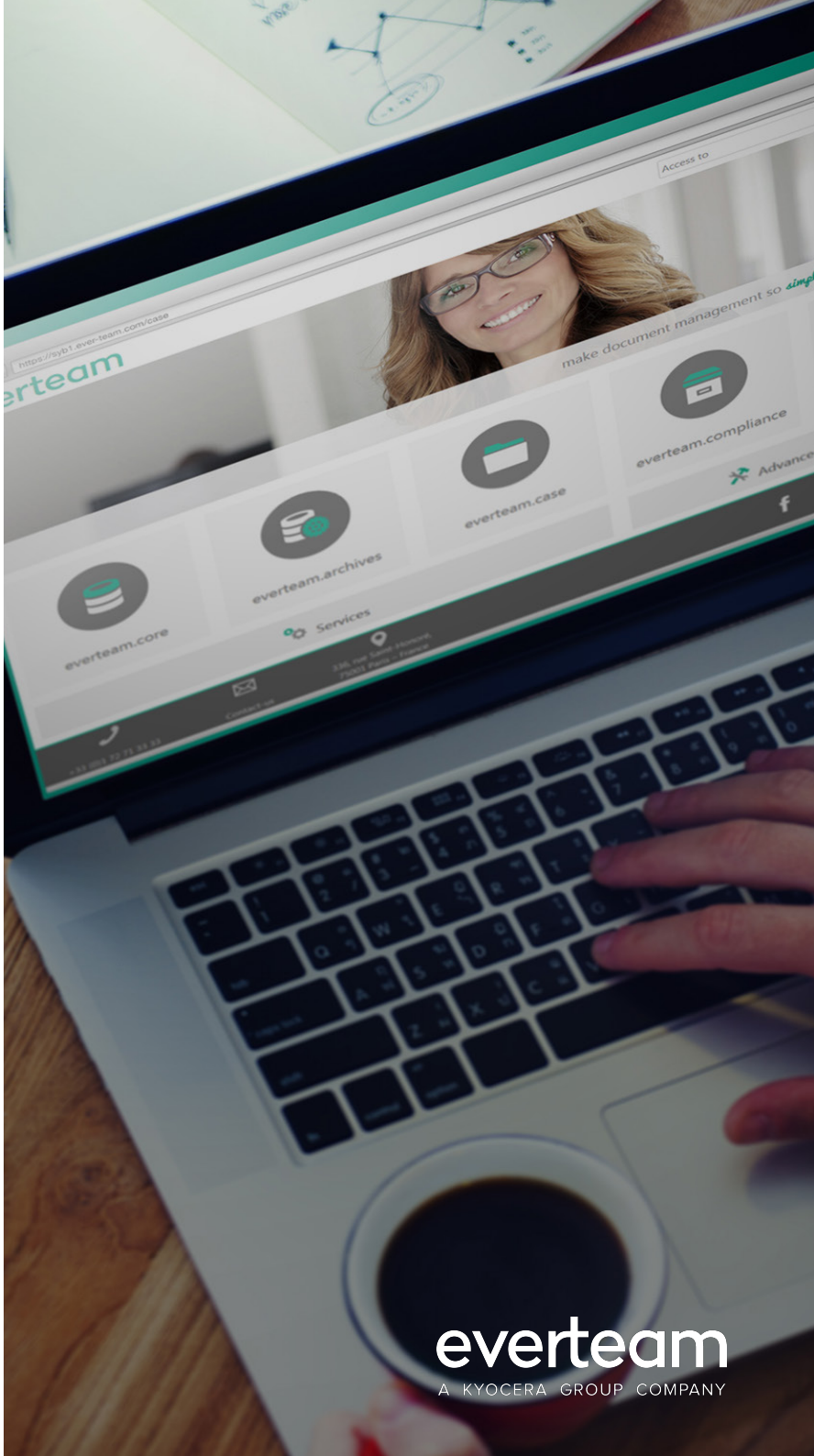
CIL et DPO, ce n’est pas (vraiment) la même chose !

... et plus de responsabilités

On estime qu’il existe, aujourd’hui, environ 4 000 Correspondants informatique et libertés en activité. Ils vivent sans doute leurs dernières heures avec l’entrée en fonction des DPO. “Les CIL et les DPO ne cohabiteront pas, confirmait ainsi, début 2016 lors de la 10ème université de l’Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP), Edouard Geffray, secrétaire général de la CNIL. Il y aura une conversion de l’un vers l’autre mais les modalités restent à fixer. Et le titre actuel de CIL ne donnera pas lieu automatiquement au titre de DPO.”

Car le DPO doit faire face à plus de responsabilités que le CIL. Sa désignation étant obligatoire dans de nombreux cas, c’est à lui de répondre en cas de contrôle opéré par la CNIL — ou par tout autre organisme de contrôle européen, la CNIL pouvant être “remplacée” par un autre si l’entreprise concernée opère principalement à l’extérieur de nos frontières. De lourdes amendes pouvant être prononcées en cas de défauts constatés, l’impact du DPO sur le destin de l’entreprise est donc incontestable !

Tous les CIL ne deviendront pas, en mai 2018, des DPO. Ces derniers doivent en effet posséder un solide bagage technique et légal pour mener à bien leurs missions. Ils n’ont pas, de plus, un simple rôle consultatif comme le CIL. Mais quel est leur profil ? Réponse dans les prochaines pages !



Le DPO, garant du RGPD

DPO : quelles qualités, quelles compétences ?

Il n'existe pas de profil-type pour devenir DPO. C'est le cas de toute nouvelle fonction, quel que soit le secteur d'activité ! Néanmoins, certaines qualités et compétences sont incontournables pour réussir dans cette mission inédite. Voici lesquelles.

Ce que dit la loi

Un grand principe régissant l'accès à la profession de DPO ? Voici :
"[Le DPO doit être désigné] sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir [ses] missions."

C'est notamment pour cela que tous les CIL ne peuvent devenir DPO. En effet, une étude menée pour la CNIL en 2015 a démontré que ceux-ci proviennent de domaines d'expertise très variés (profil technique à 47 %, en large majorité donc, profil juridique à 19 % et profil administratif à 10 %). Lesquels ne collent pas forcément tous avec les exigences liées à l'exercice du métier de DPO !

DPO : des qualités ...

La première des qualités du DPO ? La communication. Il doit en effet être capable d'expliquer à ses collaborateurs les tenants et les aboutissants de sa mission, les réorganisations nécessaires pour qu'il puisse la mener à bien, justifier les choix des outils qui vont lui permettre d'être efficace… Le DPO doit par ailleurs être rigoureux et attentif aux détails. En effet, le moindre oubli peut être considéré comme une faute par une autorité de contrôle. Mieux vaut donc ne rien laisser passer !

Ensuite, il doit savoir revendiquer son indépendance. Et faire ce qui s'impose pour qu'elle ne soit pas remise en question ! Enfin, le DPO doit être capable d'animer un réseau et une équipe. Ses responsabilités sont transverses, ce qu'on lui demande également. Un esprit tourné vers l'horizontalité et le partage, en mode "projet", semble donc incontournable !

Une autre qualité indispensable ? La curiosité, bien sûr. Et n'oubliez pas la capacité à accepter de se former régulièrement, en fonction des avancées technologiques et légales !

everteam
A KYOCERA GROUP COMPANY

Le DPO, garant du RGPD

CIL et DPO, ce n’est pas (vraiment) la même chose !

… des compétences !

Reste la question des connaissances que doit pouvoir mobiliser le DPO dans le cadre du RGPD. Selon les recommandations de la CNIL, il doit posséder :

- Une véritable expertise en matière de législation et de pratiques sur la protection des données. Son arme ? La formation continue, afin de se mettre au niveau, en temps réel, avec l’activité de son entreprise et la sensibilité des données collectées et traitées ;

- Une connaissance solide des opérations de traitement, des systèmes d’information et des logiciels utilisés dans l’entreprise. Le DPO ne doit donc pas être un novice en matière de gestion des données, et il doit avoir été sensibilisé aux questions éthiques, morales et légales soulevées par ces pratiques.

- Une compréhension des risques légaux et judiciaires encourus par l’entreprise en cas de manquement aux exigences du RGPD…

“Devenir DPO” ne s’improvise pas. On le voit, au-delà des qualités humaines, d’importantes compétences sont requises. C’est pourquoi il est capital d’anticiper l’arrivée du DPO et d’être prêt avant l’échéance du 25 mai 2018 !

Le DPO, garant du RGPD

La mission du DPO : le respect du RGPD

Maintenant que l'on en sait un peu plus sur le DPO, il est temps de parler de ses missions. Garant du respect du RGPD, il va articuler ses actions autour de trois grands principes : l'accountability, le Privacy by design, et le Privacy by default. Décryptage !

Pourquoi désigner un DPO ?

Le DPO de l'entreprise va mener à bien sa mission avec trois objectifs en tête :

- **Sécuriser juridiquement les données,** ce qui amènera à sécuriser l'activité de l'entreprise en limitant les risques de devoir assumer une amende potentiellement importante et des sanctions non-négligeables (5 ans d'emprisonnement et 300 000 euros d'amende au pénal, avec versement au civil de dommages et intérêts) pour la réputation ;

- **Valoriser le patrimoine informationnel de l'entreprise,** qui peut l'aider à grandir et à conquérir de nouveaux marchés s'il est bien exploité ;

- **Renforcer la confiance des clients et des partenaires,** en créant et en respectant une politique stricte de protection des données.

Pour cela, il dispose de trois principes qui font office de clé de voûte du RGDP : l'accountability, le Privacy by design, et le Privacy by default.

everteam
A KYOCERA GROUP COMPANY

L’accountability

Le premier grand principe du RGPD, et premier “guide” du DPO, est donc l’accountability. C’est l’article 5-2 du texte qui le rappelle. L’idée ? Selon la CNIL, il s’agit de “l’obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données”. Le DPO devra donc s’assurer que son employeur — ou celui qui lui confie sa mission, en cas d’externalisation de celle-ci — respecte bien ce principe, et d’œuvrer pour la mise en œuvre des process permettant de s’assurer de la conformité juridique des traitements, avec une traçabilité prenant effectivement une valeur probante compte tenu du renversement de la charge de la preuve.

Le Privacy by design

Le concept du Privacy by design ? Que chaque nouvelle application, chaque nouveau process, respecte bien les principes et les exigences de protection des données, dès la phase de conception. Cela implique donc que le DPO soit associé à toutes les stratégies de développement, que l’on parle d’une appli, d’un objet connecté, d’un CRM (Customer relationship manager, ou logiciel de gestion de la relation client) ou encore de n’importe quelle campagne marketing !

Le Privacy by default

Le principe du Privacy by default a pour but d’inciter le DPO à impulser une limitation des traitements de données à ce qui est strictement nécessaire. Ainsi, le garant du RGPD aura pour mission de vérifier que chaque nouveau process ne mobilise pas de données inutiles ou superflues, les conserve durant un temps raisonnable et ne les ouvre pas à n’importe qui. L’objectif ? Rassurer les consommateurs !

Le DPO, garant du RGPD

La mission du DPO : le respect du RGPD

En pratique, les missions du DPO

Reste maintenant à voir ce que, concrètement, ces missions donneront au quotidien pour le DPO. Pour le savoir, il suffit de se tourner vers l'article 39 du RGPD. Celui-ci prévoit que le Délégué aura AU MOINS les points suivants à assurer :

- "Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent (…) en matière de protection des données" ;

- "Contrôler le respect du (…) droit (…) en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant" ;

- "Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données" ;

- "Coopérer avec l'autorité de contrôle" et "Faire office de point de contact … sur les questions relatives au traitement, y compris la consultation préalable (…) et mener des consultations, le cas échéant, sur tout autre sujet" ;

- "[Tenir] dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement".

Le DPO est donc clairement au cœur de la stratégie de l'entreprise, qui se trouve renouvelée par les nouveaux impératifs du RGPD. Il doit être associé à toute décision susceptible d'impacter sur la vie privée des personnes concernées, et tout mettre en place pour leur garantir l'accès aux données que celles-ci souhaitent les modifier, les consulter, les limiter, les transférer ou les supprimer.

Rappelons une nouvelle fois que le DPO n'a pas un simple rôle de conseil comme le CIL. Et qu'en cas de contrôle faisant apparaître des manques, les sanctions tomberont : les amendes administratives pourront s'élever à 10 millions d'euros ou à 4 % du chiffre d'affaires annuel mondial de l'entreprise. Certes, la CNIL pourra se montrer conciliante les premiers temps. Mais elle n'hésitera pas à "faire des exemples", et sa clémence — largement hypothétique rappelons-le — ne durera qu'un temps !

Avec ses missions plus précises, ses responsabilités renouvelées et son rôle important dans l'opérationnel de l'entreprise, le DPO se fait incontournable avec le RGPD. Vous vous apprêtez à en devenir un vous-même (ou à en désigner un au sein de votre organisme) ? Tournez les pages pour savoir comment mener à bien vos missions !

everteam
A KYOCERA GROUP COMPANY

INCARNER LA FONCTION DE DPO

Comprendre le RGPD et s'y préparer
Top 8 des bonnes pratiques pour devenir un DPO efficace
S'assurer de sa propore indépendance en tant que DPO

www.everteam.com

everteam
A KYOCERA GROUP COMPANY

Incarner la fonction de DPO

Comprendre le RGPD et d'y préparer

En pratique, les missions du DPO

La fonction de DPO existe par et pour le respect du RGPD. Si vous vous apprêtez à l'assumer, vous devez donc tout comprendre sur ce texte novateur en matière de protection des données. Vous êtes encore un peu perdu ? Pas de panique : voici tout ce qu'il faut savoir !

Commençons par un peu d'histoire. Le RGPD va permettre de tourner la page de la directive européenne de 1995 (95/46/CE), qui régissait jusque-là l'accès des entreprises aux données personnelles. Celle-ci présentait deux problèmes majeurs. D'une part, elle avait l'objet d'une transposition dans les différents droits nationaux, créant de fait des disparités et des inégalités entre les pays et entre les entreprises. D'autre part, elle n'était pas assez dissuasive : c'est grâce à cette directive que la CNIL avait pu infliger à Google, voici quelques mois, une amende de 150 000 euros. Autant dire que c'était, pour le géant américain, exactement comme si vous vous retrouviez en tant que particulier face à une amende dont le montant était de 2 euros !

C'est notamment pour ces raisons que le législateur européen s'est attelé, voici plusieurs années, à rédiger une nouvelle réglementation : le RGPD. Sa création n'a pas été une mince affaire : lobbies de tous genres et groupements d'entreprises ont tout fait pour ralentir le processus. Mais, en avril 2016, il a enfin été voté. Pour plus d'efficacité, il n'a pas pris le statut de directive mais de règlement : c'est pour cela qu'il va s'appliquer tel quel dans l'ensemble des pays membres de l'Union européenne, sans transcription dans les droits nationaux respectifs !

Concrètement, le RGPD va changer le rapport qu'entretiennent les entreprises avec leurs données. En effet, jusqu'à présent, une déclaration préalable devait être enregistrée auprès de la CNIL. Dès le mois de mai prochain, celle-ci disparaîtra au profit de la tenue d'un registre. Avec cet ajustement, la "charge de la preuve" va être inversée.

Auparavant, la CNIL devait, après un contrôle, démontrer les manquements de l'entreprise. Le responsable du traitement avait alors du temps — quelques semaines ou quelques mois — pour régulariser. Lorsque le RGPD deviendra applicable, ce sera à l'entreprise de prouver qu'elle est en conformité en cas de vérification des traitements en cours.

everteam
A KYOCERA GROUP COMPANY

Incarner la fonction de DPO

Comprendre le RGPD et d'y préparer

6 étapes pour se mettre en conformité

Vous ne savez pas par où commencer ? La CNIL a fourni un référentiel, reposant sur 6 étapes. En tant que DPO, il vous reviendra de vous assurer que chacune d'entre elles a été suivie à la lettre. La bonne volonté et/ou la bonne foi ne suffira pas lors d'un contrôle !
Quelles sont les étapes de la mise en conformité au RGPD ? Réponse tout de suite :

Etape 1 : la désignation d'un pilote. C'est vous, en tant que DPO ! Votre mission ? Gérer la gouvernance de l'information au sein de votre entreprise. Vous aurez donc à planifier les actions destinées à appliquer le RGPD. Et ce, sans concurrence : DPO et CIL n'ont pas vocation à coexister, le premier doit remplacer le second !

Etape 2 : la cartographie. En tant que DPO, vous devrez recenser le traitement des données personnelles (finalités, sous-traitants, stockage, durée de conservation, origine et destination des données…), via un registre des traitements. Attention, l'ensemble des traitements de données personnelles devra être documenté.

Etape 3 : la priorisation des actions correctrices sur le traitement des données personnelles. Le principal critère à retenir : les risques qui pèsent sur les droits des personnes concernées. Il s'agira là de redonner le pouvoir aux particuliers sur leurs données.

Etape 4 : la gestion des risques. Immanquablement, des défauts auront été constatés dans le traitement des données. Autant de pistes pour des actions concrètes à mettre en place pour les corriger.

Etape 5 : l'organisation (ou la réorganisation des processus internes). Le RGPD va imposer aux entreprises de permettre à chacun un accès rapide aux données qui les concernent, pour qu'ils puissent les éditer, les consulter ou les supprimer. Ce qui va vous demander, en tant que DPO, de créer de nouveaux process et d'impulser l'adoption de nouveaux outils.

Etape 6 : la traçabilité. La CNIL — ou toute autre autorité de contrôle européenne — ne se gênera pas pour vérifier que la mise en conformité a bien été effectuée. Elle doit ainsi pouvoir consulter une documentation complète, actualisée régulièrement par vos soins et exportable facilement.

Incarner la fonction de DPO

Comprendre le RGPD et d'y préparer

De nouveaux droits à respecter

L'information est un véritable patrimoine. En tant que DPO, il vous reviendra de garantir aux consommateurs que leurs droits sont bien respectés et que ce "patrimoine" n'est pas illégal. Ainsi, vous devrez par exemple pouvoir assurer l'effacement des données dès lors que la personne concernée en fera la demande. On appelle cela le "droit à l'oubli", et les tribunaux européens prennent la question très au sérieux, comme en témoignent les différentes affaires jugées jusque-là ! Il vous reviendra également de permettre aux consommateurs de consulter les informations que votre entreprise possède sur eux pour, si besoin, les modifier.

Il peut s'agir de corriger :

- un nom mal orthographié ;
- une adresse incorrecte ou obsolète ;
- une composition du foyer erronée ou datée ;
- un numéro de téléphone qui a changé…

Notez que les personnes concernées auront aussi la possibilité de demander la limitation des traitements de données qui auraient été effectués avec un consentement illégal, voire de vous demander ce que vous faites des données collectées. Le RGPD vous imposera aussi de répondre favorablement aux demandes dans les meilleurs délais. Les textes officiels sont même précis sur ce point : "Un mois au plus tard après avoir pris connaissance" de la requête, selon le Règlement !

Dernier point capital du RGPD, et non des moindres : la question de la portabilité des données. En tant que DPO, vous devez en effet être en mesure de rendre les informations consultables dans un format couramment utilisé et lisible par machine. Les données communiquées devront être lisibles par n'importe quelle personne concernée, quel que soit son système d'exploitation et/ou ses équipements. Les formats propriétaires ou verrouillés seront donc à proscrire, au profit de formats plus ouverts !

Vous en savez plus sur le RGPD ? Vous avez fait le premier pas vers une bonne "incarnation" du rôle de DPO. Reste maintenant à le devenir vraiment…

everteam
A KYOCERA GROUP COMPANY

Incarner la fonction de DPO

Top 8 des bonnes pratiques pour devenir un DPO efficace

Prêt à devenir DPO ? Pas tout à fait ? Pas d'inquiétude : quelques pratiques et conseils simples vous permettront d'assurer dans vos nouvelles fonctions en quelques semaines. Voici lesquelles !

1/ Se former !

C'est le conseil le plus évident. Personne ne naît DPO. N'importe qui pourrait avoir besoin de se former sur ce nouveau métier. Plusieurs lieux d'apprentissage proposent ainsi des formations courtes — de l'ordre de quelques jours — pour comprendre les tenants et les aboutissants de cette fonction. Des formations longues, voire diplômantes, existent également. Vous pouvez également vous former seul, via des MOOCs ou des livres. Le principal ? Trouver toutes les réponses à vos questions avant de devoir être opérationnel, c'est-à-dire bien avant le mois de mai 2018 !

2/ Mettre en place une veille dynamique

Un bon DPO est un DPO informé sur les actualités liées à son activité. Organisez donc une veille (juridique, technique, sectorielle, sociétale…) sur les sujets touchant aux données à caractère personnel. Pour cela, vous pouvez utiliser les réseaux sociaux (Twitter en tête) et les outils de syndication (comme Feedly, par exemple). Abonnez-vous aux revues et aux newsletters de la CNIL et de Légifrance. Constituez une bibliographie. Et surtout, mettez tout cela à jour régulièrement — dans l'idéal, un contrôle tous les mois !

3/ Créez votre réseau

Vous ne serez pas le seul DPO de votre secteur d'activité. Guettez donc les opportunités de structurer votre réseau, d'échanger sur les bonnes pratiques et de discuter de points techniques et légaux. Les réseaux sociaux (et notamment LinkedIn, le réseau social professionnel le plus intéressant pour les profils techs) vous seront utiles, mais ils devront être complétés par des rencontres "en vrai", dans des groupes de travail, des ateliers, des réunions, des associations, des conférences… Bref, réseautez, par tous les moyens possibles !

4/ Identifiez les outils mis à votre disposition

La CNIL accompagne le déploiement du RGPD en France. Elle a, de fait, créé toute une masse d'outils pratiques pour vous aider à vous installer en tant que DPO, comme un modèle de registre des données, des guides étape par étape, des fiches d'information… Autant dire que cela vous servira régulièrement. À imprimer ou sauvegarder pour une consultation plus aisée !Le DPO est, par ailleurs, un nouveau métier. Et qui dit nouveau métier, dit aussi nouveaux outils ! Les nouvelles technologies peuvent donc vous accompagner au quotidien et vous faciliter grandement la tâche. Mais on en reparle un peu plus loin !

everteam
A KYOCERA GROUP COMPANY

5/ Rencontrez les services concernés

On l'a vu précédemment, en tant que DPO, vous allez être pleinement intégré à l'opérationnel de votre entreprise. Vous allez être impliqué dans la création de tout nouveau dispositif, produit ou opération marketing. Il est donc capital, pour que votre mission se déroule dans les meilleures conditions, de rencontrer à plusieurs reprises ceux avec lesquels vous allez travailler, que ce soit au quotidien ou de façon ponctuelle, et de collecter certaines informations. Pour cela :

- Consultez les organigrammes des directions, avec un descriptif de chaque métier ;

- Entrez en contact avec chaque responsable opérationnel. Il vous faudra en effet déterminer s'il ou elle doit traiter des données à caractère personnel.

- Organisez des rendez-vous avec chaque professionnel concerné par votre nouvelle activité. Au-delà d'une présentation et d'une première rencontre, cela vous permettra de commencer à mettre en place votre future collaboration.

6/ Réalisez un audit

Cela doit être l'une de vos premières actions en tant que DPO. Réaliser un audit vous permettra d'identifier l'ensemble des traitements de données personnelles en cours dans votre entreprise. Vous saurez également quelles sont les informations collectées : le nom, le prénom, le numéro de téléphone, l'adresse postale, le mail, l'historique des achats… Cela vous permettra de commencer à créer votre plan d'action et à évaluer le niveau de conformité de votre organisme.

7/ Plongez-vous dans le RGPD

Le RGPD dans son intégralité, c'est 99 articles et plus de 170 considérants. Soit plus de 60 pages de textes législatifs, parfois obscurs. Bref, cela ne donne pas envie d'en faire sa lecture du soir ! Et pourtant, vous n'y couperez pas : vous allez devoir tout lire, ligne par ligne. En effet, il comporte probablement des particularités propres à votre secteur d'activité vous autorisant — ou vous interdisant — certains traitements ou vous imposant certaines demandes d'autorisation. Passer à côté de ces dispositions, ce serait se mettre hors-la-loi. Et la CNIL ne vous le pardonnerait pas !

8/ Communiquez en interne

Le DPO est le chef d'orchestre de l'application du RGPD en entreprise. Veillez donc à avoir les moyens (financiers, humains, techniques et opérationnels) pour communiquer en interne sur la problématique de la protection des données. Plus vos collaborateurs seront sensibilisés, moins vous aurez, dans la durée, d'actions correctrices à mettre en place. Un exemple d'idée ? Une newsletter bimensuelle, pour expliquer votre métier et vos décisions !

Un dernier conseil ? Veillez à votre indépendance. Pour savoir comment, consultez le chapitre suivant !

everteam
A KYOCERA GROUP COMPANY

Incarner la fonction de DPO

S’assurer de sa propre indépendance en tant que DPO

L’indépendance du DPO est une condition sine qua none pour qu’il puisse assurer sa mission dans de parfaites conditions. Ainsi, vous devez vous assurer que certaines conditions seront bien remplies. Lesquelles ? Comment s’y prendre ? Comment éviter tout conflit d’intérêts ? Réponse tout de suite !

La nécessaire absence de sanctions

C’est l’un des principaux points auxquels il vous faudra veiller : bénéficier d’une protection suffisante dans votre quotidien et ne pas vous faire sanctionner pour une décision prise ou un conseil donné. Ainsi, le Règlement est très clair : “Le DPO ne peut être relevé de ses fonctions ou pénalisé par le responsable de traitement ou le sous-traitant pour l’exercice de ses missions.”

Un exemple ? Vous serez peut-être amené à conseiller au responsable de traitement de procéder à une analyse d’impact, si vous constatez qu’un traitement présente des risques élevés. En cas de désaccord, il ne serait pas acceptable d’être relevé de vos fonctions ou d’être sanctionné. Et les sanctions peuvent prendre diverses formes : absence de promotion ou de retard dans la promotion, freins à l’avancement de carrière, refus de l’octroi d’avantages dont bénéficient d’autres employés… Vous avez un doute, une crainte, durant votre carrière de DPO ? N’hésitez jamais à en parler à votre direction générale, voire à consulter un avocat !

Attention, ces dispositions ne font pas du DPO un “salarié protégé” au sens du Code du travail, comme peuvent l’être, par exemple, les délégués syndicaux. Ainsi, les autres motifs de licenciement légitime (vol, harcèlement physique, sexuel ou moral, fautes professionnelles lourdes…) peuvent s’appliquer !

L’absence de conflits d’intérêts

En tant que DPO, vous devez veiller à ne jamais être juge et partie. C’est ce que l’on appelle “veiller à l’absence de conflit d’intérêts”. Le plus simple ? Évitez d’occuper (et renoncez le cas échéant) l’une des fonctions suivantes au sein de votre entreprise :

- Secrétaire général ;
- Directeur général des services ;
- Directeur général ;
- Directeur opérationnel ;
- Directeur financier ;
- médecin-chef ;
- Responsable du département marketing ;
- Responsable des ressources humaines ;
- Responsable du service informatique…

Attention, la CNIL se posera systématiquement, en cas de contrôle, la question de la présence ou non d’un conflit d’intérêts. L’appréciation se fera au cas par cas !

everteam
A KYOCERA GROUP COMPANY

Incarner la fonction de DPO

S’assurer de sa propre indépendance en tant que DPO

Le DPO n’est pas plus responsable pénalement que le CIL

La question de la responsabilité pénale est importante. En cas de manquement aux obligations du RGPD, le DPO est-il “coupable” ? À cette question, la Commission européenne a répondu… non, pas plus que le CIL ne l’était jusqu’à présent. C’est en effet le responsable du traitement ou le sous-traitant qui pourrait avoir à répondre, devant les tribunaux, de pratiques non-conformes. C’est aussi lui qui doit démontrer que le traitement est effectué conformément aux dispositions du RGPD.

Une exception toutefois : la responsabilité pénale du DPO peut être engagée s’il enfreint intentionnellement les dispositions du RGPD. C’était le cas du CIL avec la loi Informatique et Libertés, cela ne change donc pas avec le DPO !

Indépendance, absence de conflit d’intérêts et responsabilité partagée constituent les maîtres mots d’une action sereine du DPO. Posez-vous régulièrement la question suivante : “Les conditions d’exercice de ma fonction sont-elles respectées ?”

LES OUTILS ET LE QUOTIDIEN DU DPO

Le Big Data et le Machine Learning au secours du DPO
La boîte à outils du DPO

www.everteam.com

everteam
A KYOCERA GROUP COMPANY

Les outils et le quotidien du DPO

Le Big Data et le Machine Learning au secours du DPO

Le nouveau Règlement général sur la protection des données va modifier en profondeur l'organisation des entreprises. Leurs rapports aux données générées et aux process vont également changer, tendant vers plus de transparence… et d'efficacité. Tout cela va nécessiter de mettre en place certains outils — dont nous parlerons ensuite. Reste que des technologies seront précieuses pour vous aider dans votre quotidien : le Big Data et le Machine Learning.

Big Data, Machine Learning : quèsaco ?

Commençons par bien définir ce dont nous allons parler dans cette partie. Le Big Data constitue une réponse à l'explosion récente constatée du volume d'informations. Il va donc regrouper certains outils répondant à trois problématiques (connues sous l'appellation "3V") :

- Un Volume inédit de données, qui doivent être traitées pour être valorisées ;
- Une grande Variété des informations, issues de plusieurs sources, souvent non-structurées et de formats différents ;
- Une Vitesse de création des données jamais atteinte jusqu'à présent nécessitant une collecte et une analyse tout aussi efficace.

Et le Machine Learning ? Il s'agit d'un processus de fonctionnement d'un système d'IA (Intelligence artificielle), lui permettant d'acquérir des connaissances, de prendre des décisions et de nouveaux réflexes. L'objectif ? Optimiser les tâches, aller plus vite et se servir de l'apport du Machine Learning pour reconnaître certaines situations et effectuer automatiquement des déductions et des opérations !

Les apports du machine learning

En tant que DPO, vous aurez à répondre à certaines sollicitations de la part des personnes concernées, ou du moins à organiser l'entreprise pour qu'elle soit en mesure d'y répondre. Il pourra, rappelons-le, s'agir de consulter une donnée, de la modifier ou encore de la supprimer, et ce dans des délais raisonnables — de l'ordre de quelques jours (30 tout au plus).

Autant dire que la tâche pourra sembler bien fastidieuse, et les délais difficilement tenables, avec des solutions "classiques" et non optimisées de gestion des données. La solution ? Le recours à des logiciels de gouvernance de l'information intégrant une double dimension "Big Data" et "machine learning", afin de gagner en efficacité au quotidien.

L'objectif ? Pouvoir identifier la donnée rapidement. Mieux : l'identifier de plus en plus vite au fur et à mesure de l'utilisation de la solution. Mais aussi automatiser les process et répondre avec plus d'efficacité aux demandes (limitation, rectification, anonymisation, suppression) des personnes concernées. Ce qui, au passage, permettrait d'enrichir automatiquement le registre de traitement, que la CNIL doit pouvoir consulter !

Machine Learning et Big Data viennent donc en soutien des DPO. Sans ces dimensions, les outils ne sont pas vraiment utiles. Ils rendent la tâche fastidieuse et plus longue qu'elle ne pourrait l'être !

Les outils et le quotidien du DPO

La boîte à outils du DPO

En tant que DPO, vous allez devoir composer avec un quotidien fait d'anticipations, d'accompagnements, de vérifications, de mesures correctrices, de communications et d'informations. Autant dire que l'appui de certains outils deviendra vite incontournable pour maximiser l'efficacité de votre gouvernance de l'information. Voici une petite sélection, à conserver à l'esprit !

Les outils… mis à disposition par la CNIL

La CNIL est le premier acteur à même d'aider les entreprises et les DPO à organiser leurs missions. C'est pourquoi l'autorité de régulation a créé plusieurs outils, pratiques et concrets, pour savoir ce qu'il faut faire et à quel moment.

Le premier outil ? Des packs de conformité sectorielle. "Ils visent à définir et diffuser les bonnes pratiques pour un secteur, tout en simplifiant les formalités administratives des acteurs qui s'y conforment, indique la CNIL. Ils peuvent ainsi contenir des mesures de simplification des formalités, des guides pratiques et pédagogiques, des tests de vérification de conformité à la loi." Pour l'heure, trois packs sectoriels ont été créés : "compteurs communicants", "logement social", "assurance" et "véhicules connectés". D'autres devraient arriver dans les prochaines semaines, afin de répondre à un maximum de problématiques précises !

La CNIL propose également, sur son site, un modèle de registre de traitement au format Excel, ainsi qu'un guide pratique sur le RGPD. À conserver dans un coin de son navigateur Web.

Les outils pour… la gouvernance de l'information

Que l'on se trouve dans une TPE/PME ou dans un grand groupe, le DPO ne pourra pas exercer ses missions sans un logiciel automatisé de gestion des données personnelles. Ce type de programme permet notamment :

- De lister les traitements automatisés ;
- De créer une base documentaire mise à jour en temps réel ;
- D'identifier là où se trouvent les données sensibles dans les ensembles non-structurés comme structurés, pour y accéder plus facilement et mener les éventuelles opérations correctives ;
- De cartographier l'ensemble des traitements ;
- De tenir le registre des traitements ;
- D'éditer un bilan annuel, qui pourrait être demandé par la CNIL en cas de contrôle ;
- De gérer l'ensemble des tâches demandées par les consommateurs (consultation, suppression, modification, anonymisation)…

Notons et saluons particulièrement l'outil PIA mis à disposition par la CNIL (https://www.cnil.fr/fr/rgpd-un-logiciel-pour-realiser-son-analyse-dimpact-sur-la-protection-des-donnees-pia)

Dans les plus grandes structures, il peut être intéressant de compléter ce type de logiciel par d'autres composants logiciels d'analyse de contenu.. A ce titre, Everteam propose, notamment, des outils de "file analysis" dédiés à l'analyse de contenu "non structuré" ou "semi structuré". Ces outils automatiques combinent des fonction de NLP (Natural Language Processing), d'auto-classification, d'archivage et de gouvernance de l'information, utiles pour accéder plus vite et plus précisément à son capital informationnel et en appréhender la valeur et les risques associés. Ces fonctionnalités sont particulièrement précieuses pour les DPO :

- Indexation automatique des caractéristiques techniques des fichiers, par date de création et de dernier accès, format, taille, langue et arbre de classification ;
- Analyse du contenu des documents en vu d'identifier automatiquement les données personnelles;
- Renforcement des mesures de prévention des risques (cloisonnement, archivage, minimisation de la donnée, chiffrement,...) ;
- Réalisation automatique d'actions pré-configurées, optimisées au fur et à mesure de l'apprentissage par le logiciel…

Ce type de logiciels vous permettra de disposer d'un point d'accès centralisé pour rechercher une information suite à une sollicitation de la part des personnes concernées ou de la CNIL. Qualifiée plus tôt, l'information disposera ainsi d'un cycle de vie mieux maîtrisé et ne sera conservée que si elle est utile. Autant d'impératifs explicitement exprimés dans le RGPD ! Enfin, ils vous assureront de répondre rapidement aux demandes en cas d'audit ou de contrôle, et de prouver la fiabilité et l'intégrité de votre système d'information. Précieux !

Les outils ... pour communiquer

Le “DPO prêt à l’action” que nous appelons de nos vœux dans ce Livre Blanc est aussi un DPO qui sait communiquer en interne. C’est pourquoi il est important de vous rappeler les outils qui vous permettront d’échanger avec vos collaborateurs, au quotidien comme en mode “gestion de projets”.

Vous pouvez par exemple adopter un outil de discussion instantanée en ligne en Intranet. En créant des “channels”, vous pourrez échanger des messages en temps réel avec l’ensemble des professionnels impliqués dans la gouvernance de l’information. Cela pourrait donc être le bon endroit pour rappeler des bonnes pratiques, prendre des nouvelles de l’avancée d’un projet, échanger sur les évolutions réglementaires… Notez que vous pouvez également y gérer des discussions privées, ouvertes à quelques personnes seulement. Pratique !

Lorsque vous aurez mis en place des projets d’évolution, il sera important en tant que DPO de disposer d’une vision globale sur les actions en cours. Qui fait quoi ? Où en est l’équipe ? Qu’est-ce qu’il reste à faire ? Nous vous conseillons pour cela d’adopter un logiciel de gestion de projet, type Trello. Fonctionnant par “planches”, il aide à savoir à quel point les dossiers avancent, et permet de confier à certains collaborateurs des tâches à accomplir.

Les outils ... pour progresser

En tant que DPO, vous devrez faire preuve de flexibilité et d’adaptabilité. C’est pourquoi il est capital de veiller à progresser constamment dans votre politique de gestion des données. Comment ? Par des formations tout d’abord. Plusieurs cours, en ligne ou en présentiel, sont d’ores et déjà proposés. Il sera important de rester up to date, et de vérifier régulièrement si de nouveaux savoirs ne sont pas indispensables à votre métier !
Ensuite, n’hésitez pas à vous faire accompagner dans votre prise de fonction et/ou dans le respect des exigences du RGPD dans votre entreprise par un intervenant extérieur. Celui-ci pourra vous aider à prioriser les actions à mettre en place, à savoir où vous en êtes, et à choisir les bons outils. Pensez-y !

La boîte à outils du DPO dépend forcément de la taille de l’entreprise et des enjeux auxquels elle est confrontée… ainsi que du volume de données à traiter. Les logiciels de traitement des données paraissent cependant incontournables, tout comme ceux de communication interne. Tous vous aideront en tout cas à tenir votre registre, dont nous allons parler tout de suite !

everteam
A KYOCERA GROUP COMPANY

Les outils et le quotidien du DPO

La tenue d'un registre

Parmi les responsabilités du DPO, on trouve la tenue d'un registre des activités de traitement. Que doit-il contenir ? Voyons cela !

L'importance du registre

Le registre de traitement est un document capital pour le respect du RGPD. Il en constitue même la pierre angulaire. La preuve ? En cas de contrôle, c'est lui qui prouvera la conformité de l'organisation. Il servira de point de départ à d'éventuels contrôles plus poussés par la CNIL. Il est donc à ne pas négliger, et doit contenir certaines informations bien précises !

Que doit contenir le registre ?

Pour connaître la réponse à cette question, c'est l'article 30 du RGPD qu'il convient d'examiner. Ainsi, le registre doit comporter l'ensemble des informations suivantes :

1/ Le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

2/ Les finalités du traitement (par exemple, "Données traitées pour communiquer mensuellement sur nos actualités d'entreprise", "prospection"…)

3/ Une description des catégories de personnes concernées et des catégories de données à caractère personnel utilisées (par exemple, "Clients ayant commandé au moins une fois un de nos produits", et "nom, prénom et email") ;

4/ Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en France comme à l'international (par exemple, "envoi par courrier", "envoi par mail", "appels téléphoniques"…) ;

5/ La mention, le cas échéant, de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale. L'identification de ce pays tiers ou de cette organisation internationale doit être explicitée et des documents prouvant que la confidentialité des données sera respectée par ceux-ci doivent être produits ;

6/ Les délais prévus pour l'effacement et/ou la modification des différentes catégories de données ;

7/ Les garanties de sécurité intégrées au traitement des données (certifications obtenues, résultats d'audits ou encore attestations des éditeurs de logiciels)…

everteam
A KYOCERA GROUP COMPANY

Les outils et le quotidien du DPO

La tenue d'un registre

6 questions à se poser

Comment s'assurer de la bonne tenue du registre ? La CNIL recommande de se poser 6 questions pour chaque traitement de données personnelles, afin de remplir les bonnes cases et de n'oublier aucune information :

Qui ?, pour inscrire les noms et coordonnées des responsables du traitement, des services opérationnels et des sous-traitants ;

Quoi ?, pour inscrire les catégories de données traitées et identifier les risques et la sensibilité de celles-ci ;

Pourquoi ?, pour être au clair sur la finalité de la collecte des données ;

Où ?, pour déterminer l'endroit où les données sont hébergées et les pays éventuels vers lesquels elles sont envoyées ;

Jusqu'à quand ?, pour mentionner clairement dans le registre la durée de conservation des données ;

Comment ?, pour connaître les mesures de sécurité mises en œuvre pour minimiser les risques !

En cas de contrôle, n'oubliez jamais que le registre sera le document demandé en premier par la CNIL, et qu'il permettra au minimum de prouver votre bonne foi. Mais d'ailleurs, que faire en cas de contrôle ? On en parle immédiatement !

Les outils et le quotidien du DPO

Que faire en cas de contrôle ?

Les premiers contrôles (réalisés sur place ou en ligne), qu'ils soient menés directement par la CNIL ou par l'équivalent dans un pays européen de cette organisation, peuvent potentiellement se tenir à partir du 25 mai 2018. Les risques financiers (jusqu'à 4 % du chiffre d'affaires global du groupe !) sont importants. C'est pourquoi il est capital d'être au clair sur le déroulement d'une telle opération, et sur ce que vous devez faire si votre gouvernance de l'information est remise en question.

Les labels CNIL mis à jour

En cas de contrôle, la CNIL va chercher à vérifier si votre politique de gestion des données est conforme au droit européen. Elle va à la fois s'assurer de votre bonne foi (vous pouvez avoir un peu de retard dans la mise en place des outils et des process, mais vous devez au moins être "sur le bon chemin") et du respect de ses impératifs en matière de protection des données personnelles.

Pour cela, il peut être intéressant de se tourner dès à présent vers les labels CNIL, mis à jour récemment avec les obligations liées au RGPD, l'autorité de contrôle assurant que "l'obtention d'un label peut servir d'élément à son titulaire pour démontrer qu'il respecte le règlement". Ainsi, la CNIL a d'ores et déjà actualisé ses référentiels "Formations" et "Gouvernance Informatique et Libertés" pour qu'ils correspondent aux exigences du RGPD.

"Les entreprises françaises ayant déjà intégré ces outils pourront aborder plus sereinement l'entrée en application du règlement puisqu'elles auront déjà fait une bonne partie du chemin vers l'accountability, clé de voûte de la conformité à l'heure du règlement", indique la CNIL. Autant dire que cela vaut le coup de se renseigner !

Les outils et le quotidien du DPO

Que faire en cas de contrôle ?

Comment se passe un contrôle ?

Aïe, la CNIL s'intéresse de près à votre gouvernance de l'information ? Il va falloir montrer patte blanche. La délégation de l'autorité de contrôle se composera d'au moins 2 membres, dont un expert technique. Ils chercheront à obtenir un maximum d'informations (techniques comme juridiques) pour déterminer dans quelles conditions vous protégez les données à caractère personnel. Ils pourront ainsi accéder aux programmes informatiques, à la data en circulation dans le SI, aux contrats signés avec des prestataires et/ou des sous-traitants, ou à n'importe quel document qu'ils estiment nécessaires pour mener à bien leurs missions.

Comment réagir ?

Ouvrez grand vos portes à la CNIL ! Rappelons que l'entrave à l'action de l'autorité de contrôle est punie d'un an d'emprisonnement et de 15 000 euros d'amende. Présentez votre registre de traitement, document centralisant l'ensemble de vos actions en matière de données personnelles. Répondez, bien sûr, à toutes les interrogations. Si besoin, faites-vous assister d'un avocat — que vous ayez, ou non, des choses à vous reprocher, la présence d'un conseil n'étant pas considérée par la CNIL comme un élément de nature à l'inquiéter…

En cas de contrôle, produisez en tant que DPO un maximum de documents démontrant que vous respectez bien les impératifs du RGPD. La CNIL vous communiquera ensuite, par courrier, l'ensemble des décisions prises à votre encontre et/ou des recommandations formulées concernant votre gouvernance de l'information.

Conclusion

Le rôle du DPO est central dans l'application, en entreprise, du RGPD. Il en est le véritable chef d'orchestre, celui qui va impulser le respect du Règlement et être l'interlocuteur des autorités. C'est pourquoi il est capital de bien se préparer à une telle fonction, notamment par une ou plusieurs formations. C'est d'autant plus vrai que certaines respecteront, dans les prochains mois, le référentiel "Formation informatique et libertés", qui permet de proposer des formations labellisées concernant le règlement européen.

Bien préparé, le "parfait DPO" évoqué dans ce Livre Blanc est aussi celui qui a adopté les bons outils en fonction de la taille de son entreprise. Rendus plus efficaces grâce, par exemple, au Machine Learning et au Big Data, ceux-ci lui permettent de gagner du temps au quotidien, de répondre favorablement aux demandes des consommateurs, et de sécuriser les données que ces derniers acceptent de communiquer. Ils mettent fin à une période "floue" en matière de gestion des données. Bref, ils rendent le pouvoir sur leurs data à ceux qui en sont les véritables propriétaires… exactement comme ce qu'exige le RGPD !

Enfin, en tant que DPO, n'oubliez pas qu'il sera de votre responsabilité d'organiser la tenue d'un registre de traitement des données. Ce document sera votre "Bible", votre référence. Il vous sera demandé en cas de contrôle. Il devra contenir l'ensemble des informations qui concernent votre politique de gouvernance de l'information.
Vous en savez maintenant plus sur ce que l'on entend par "parfait DPO". Bien sûr, des ajustements devront être opérés dans votre stratégie, avant et après l'entrée en vigueur du RGPD le 25 mai 2018. Mais c'est aussi ça qui fait qu'un DPO est idéal ou non : la capacité à s'adapter, à être flexible et réactif !

Un grand merci à Aissatou Sarr, DPO du groupe be-ys (Almerys) pour avoir contribué à ce livre blanc et partagé son expertise en tant que DPO.

A propos d'Everteam

Présent sur les 5 continents, Everteam est un éditeur de logiciels spécialisé dans la gestion de contenu d'entreprise (ECM) et la gouvernance de l'information. Son expertise et ses solutions sont centrées autour des technologies big data et adaptées à différents contextes métier.

Pour en savoir plus :
www.everteam.com
ou contactez-nous directement par mail :
info@everteam.com

Faire une demande de démo

everteam
A KYOCERA GROUP COMPANY