clubdesacheteurs

Petit-déjeuner 25 janvier 2018

Bien se préparer au RGPD

Agenda 2018

PETITS-DÉJEUNERS

Jeudi 5 juillet - **“Co-développement / co-innovation : cas concrets dans la PI”**
Mardi 25 septembre - **“Contrats d’achat télécom”**
Mardi 11 décembre - **“Sourcing PI en mode agile”**

CONFÉRENCES

Jeudi 22 mars - **“Comment les achats font-ils entrer l’innovation dans l’entreprise?”**
Mardi 5 juin - **“Centres de services : focus sur les bonnes pratiques”**
Jeudi 8 novembre - **“Innovations sur le sujet du référencement”**

AUTOMNE 2018

2ème édition du Baromètre des Achats de Prestations Intellectuelles

Nos partenaires

Décision-Achats.fr

Magazine d'information des acheteurs privé / public
Un an d'abonnement offert aux adhérents du Club des Acheteurs.

AVOCATS

Avocat au barreau de Paris depuis 15 ans, Maître Franklin Brousse est spécialisé dans l'achat de prestations intellectuelles.

PAC
A CXP GROUP COMPANY

CABINET PAC (PIERRE AUDOIN CONSULTANTS), spécialiste de l'analyse des marchés IT et des études de TJM

L’adhésion au Club des Acheteurs

4 **conférences** plénières par an suivies d'un cocktail déjeunatoire.

4 **petits-déjeuners** thématiques, témoignages et débats de Directions Achats.

Des **échanges** avec plus de 60 directions achats issues de grandes sociétés et organismes publics français.

Le **calendrier** des thématiques annuelles et l'accès à la **docuthèque** du Club.

Nouveau : l'accès en ligne aux **documents légaux** obligatoires certifiés conformes (Kbis, URSSAF, etc.) de vos fournisseurs tous secteurs d'activité confondus dans une limite de volumétrie.

Accès à l'**annuaire** en ligne des adhérents du Club.

Un **abonnement** d'un an à Décision-Achats magazine (mensuel spécialisé dans les achats).

Une **remise de 40%** pour tout participant supplémentaire.

Bien se préparer au RGPD

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL
du 27 avril 2016
relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Par Maître Franklin BROUSSE
L'Avocat des Directions Achats et des Directions Digitales

RGPD

+ Qui est concerné par ce Règlement ?

□ les entreprises
□ les organismes publics
✓ tout le monde
□ les réseaux sociaux

+ Le RGPD s'applique-t-il aux traitements des données personnelles :

□ réalisés au sein de l'Union Européenne
□ en dehors de l'Union Européenne,
✓ les deux

+ C'est quoi un responsable du traitement ?
□ une personne ou une entité qui traite des données personnelles
✓ une en personne ou une entité qui détermine les finalités et les moyens du traitement des données personnelles

RGPD

+ Qui peut être considéré comme un responsable du traitement ? (un seul choix)

□ celui qui entre des données dans un logiciel
□ celui qui collecte des données personnelles pour le compte d'un tiers
□ celui qui traite des données personnelles pour le compte d'un tiers
✓ celui détermine les moyens de collecte des données personnelles et la finalité du traitement des données personnelles

+ Laquelle de ses activités correspond à un traitement de données personnelles ? (plusieurs choix)

✓ un annuaire d'entreprise
□ un carnet d'adresses personnel
✓ une base de données des clients d'une entreprise
✓ la gestion des salariés

RGPD

+ C’est quoi un sous-traitant au sens du RGPD ?

□ celui qui entre des données dans un logiciel
✓ celui qui traite des données personnelles pour le compte d’un tiers
□ celui détermine les moyens de collecte des données personnelles et la finalité du traitement des données personnelles

+ Au fait c’est quoi une donnée personnelle ?
+ toute information relative à une personne physique identifiée ou susceptible d'être identifiée, directement ou indirectement

+ Et les mesures de protection ?
+ Le responsable du traitement met en œuvre des mesures techniques et organisationnelles de protection des données afin de répondre aux exigences du RGPD et protéger les droits de la personne concerné

+ Solution du chiffrement
+ Anonymisation
+ Pseudonymisation

Impact du RGPD sur les acheteurs

+ Dès lors qu'ils concernent l'utilisation de données personnelles toute opération ou projet implique un traitement de données personnelles.

+ Cela concerne généralement la gestion des relations avec les salariés, les clients et les fournisseurs (CRM, ERP, PAYE, SI ACHAT)

+ Evaluation préalable systématique :

+ en cas de risque potentiel : analyse d'impact relative à la protection des données
+ en cas de risque élevé avéré : consultation préalable de la CNIL

+ Un nouveau référent/intervenant dans le process achat : le délégué à la protection des données

Impact du RGPD sur les acheteurs

+ Impact sur le process d'achats :

+ identifier en amont si l'achat de prestations implique l'accès et/ou le traitement de données personnelles par le prestataire

+ Trois types de situations :

+ le prestataire a uniquement accès aux données personnelles

+ le prestataire héberge des données personnelles

+ le prestataire traite des données personnelles dans le cadre de son service

Impact du RGPD sur les acheteurs

+ Trois types de situations :

➢ le prestataire a uniquement accès aux données personnelles
+ enjeux de confidentialité et de sécurité lié à l'accès et à la consultation
+ pas sous-traitant au sens du RGPD
+ ex : Conseil / Projet de développement / Maintenance

➢ le prestataire héberge des données personnelles
+ enjeux de confidentialité, de sécurité et de conformité
+ sous-traitant au sens du RGPD
+ ex : hébergement / infogérance

➢ le prestataire traite des données personnelles dans le cadre de son service
+ enjeux de confidentialité, de sécurité et de conformité
+ sous-traitant au sens du RGPD
+ « spécificité » dans la plupart des cas : le sous-traitant de second rang
+ ex : service SaaS

Impact du RGPD sur les acheteurs

+ Enjeux de conformité au niveau des achats

+ Vérifier que les obligations du sous-traitant sont décrites au sein du contrat

+ Le contrat doit définir :

+ l'objet et la durée du traitement,
+ la nature et la finalité du traitement,
+ le type de données personnelles et les catégories de personnes concernées,
+ si le sous-traitant fait appel à un autre sous-traitant
+ si des mesures de protection des données sont spécifiquement définies
+ de manière générale toutes les obligations du sous-traitant au titre du RGPD

Impact du RGPD sur les acheteurs

+ Obligations du sous-traitant au titre du RGPD

+ ne traiter les données que sur instruction documentée du responsable du traitement
+ veiller à ce que les personnes autorisées à traiter les données s'engagent à respecter la confidentialité ou soient soumises à une obligation légale de confidentialité
+ prendre toutes les mesures requises pour garantir un niveau de sécurité adapté au risque
+ aider le responsable du traitement à s'acquitter de son obligation de traiter les demandes des personnes concernant leurs données
+ aider le responsable du traitement à garantir le respect de ses obligations en matière de sécurité
+ aider le responsable du traitement à garantir le respect de ses obligations en matière de notification et de communications en cas d'atteintes aux données personnelles
+ aider le responsable du traitement à garantir le respect de ses obligations en matière d'analyse d'impact relative à la protection des données
+ aider le responsable du traitement à garantir le respect de ses obligations en matière de consultation préalable de la CNIL
+ ne pas sous-traiter sans autorisation écrite préalable du responsable du traitement

Impact du RGPD sur les acheteurs

+ En pratique, où peuvent être définies les obligations du sous-traitant au titre du RGPD

+ dans une clause dans le corps du contrat
+ dans une ou plusieurs annexes
+ Data Processing Agreement
+ Politique de protection des données personnelles
+ dans un avenant (pour les contrats en cours d'exécution)

+ Prévenir l'avalanche des avenants à venir …
+ identifier tous les contrats où les prestataires ont la qualité de sous-traitants
+ établir un modèle d'avenant type

Impact du RGPD sur les acheteurs

+ Quel plan d'actions pour les donneurs d'ordre ?

+ identifier tous les contrats où les prestataires ont la qualité de sous-traitants et font appel à des sous-traitants de second rang
+ vérifier l'existence des engagements pris entre les sous-traitants de second rang
+ établir un modèle d'avenant type
+ établir un modèle de Data Processing Agreement
+ établir un modèle de Politique de protection des données personnelles
+ mettre à jour vos modèles de contrats / CG
+ mettre à jour votre charte informatique à destination des prestataires
+ Créer un registre « Sous-traitants » (liste des traitements effectués pour votre compte)
+ Coordonner vos actions avec votre délégué à la protection des données

+ ATTENTION : ces actions ne visent que vos relations avec les sous-traitants
+ toutes les autres obligations du responsable du traitement

Impact du RGPD sur les acheteurs

+ Pourquoi est-il nécessaire de se conformer avant le 25 mai 2018 ?

+ la menace de sanctions lourdes

+ En cas de manquement aux obligations du responsable du traitement
+ les amendes administratives jusqu'à 10 000 000€ ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent d'une entreprise

+ En cas de manquement aux principes de base d'un traitement de données, aux droits des personnes au transfert de données ou de non-respect des injonctions de la CNIL
+ les amendes administratives jusqu'à 20 000 000€ ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent d'une entreprise

Impact du RGPD sur les acheteurs

+ Pourquoi est-il nécessaire de se conformer avant le 25 mai 2018 ?

+ les dernières sanctions avant RGPD

+ la CNIL vient de rendre deux décisions condamnant Hertz et Darty à de lourdes amendes (40 000 € pour Hertz et 100 000€ pour Darty).

+ CNIL prononce une sanction de 100 000 euros à l'encontre de DARTY pour ne pas avoir suffisamment sécurisé les données de clients ayant effectué une demande en ligne de service après-vente

+ le fait de faire appel à un prestataire sous-traitant ne décharge pas de son obligation de préserver la sécurité des données traitées pour son compte, en sa qualité de responsable du traitement.

Impact du RGPD sur les acheteurs

+ Que va faire la CNIL dans les prochains mois ?

+ contrôler l'application du RGPD et veille au respect de celui-ci

+ encourager la sensibilisation des responsables du traitement et des sous-traitants

+ encourager la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données

+ publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

+ publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise

Impact du RGPD sur les acheteurs

+ Que va faire la CNIL dans les prochains mois ?

+ adopter des clauses contractuelles types pour les contrats avec les sous-traitants

+ publier les critères d'agrément d'un organisme chargé du suivi des codes de conduite (*Les associations et autres organismes professionnels qui ont l'intention d'élaborer un code de conduite ou de modifier ou proroger un code de conduite existant soumettent leur projet de code à la CNIL*)

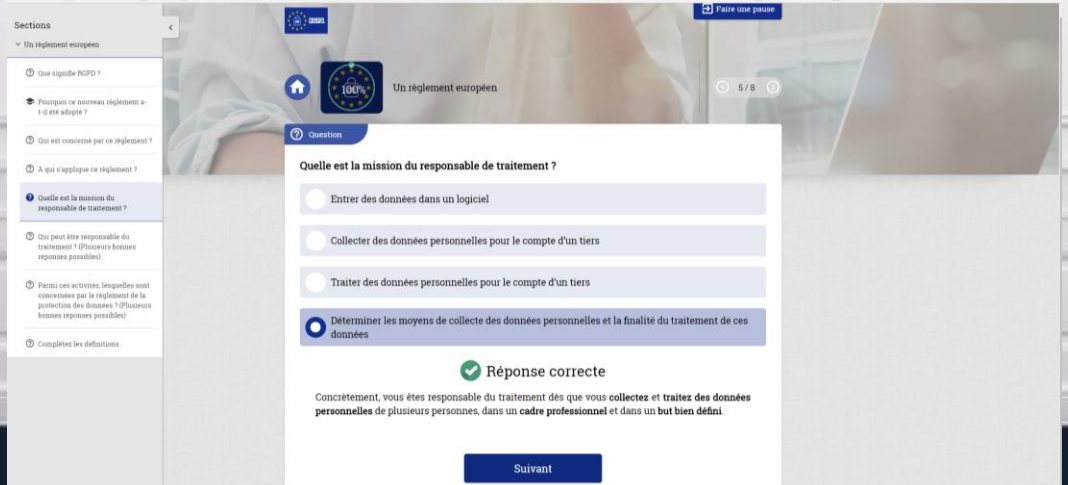
+ agréer des organismes de certification et les organismes chargé du suivi des codes de conduite

+ rendre un avis sur les projets de codes de conduite et approuver ceux qui seront conformes

Impact du RGPD sur les acheteurs

+ RGPD : Nouveau risque ou nouvelle opportunité pour les acheteurs ?
+ un risque supplémentaire à intégrer dans le process achat
+ une opportunité supplémentaire de renforcer la place de l'acheteur au cœur du process de contractualisation

+ Se faire accompagner et se former pour pouvoir profiter de cette opportunité
+ Quelle solution de formation ? Micro e-learning



Actualités

+ **<u>Création d'un outil de micro e-learning pour sensibiliser les non juristes au RGPD</u>**

+ Le cabinet a participé en 2017 à la contractualisation de plus de 80 000 000€ d'achats informatiques, télécoms, logistiques et marketing.

+ La cartographie des principaux risques juridiques liés aux achats indirects

+ Le programme de formation juridique sur mesure pour les acheteurs et les juristes