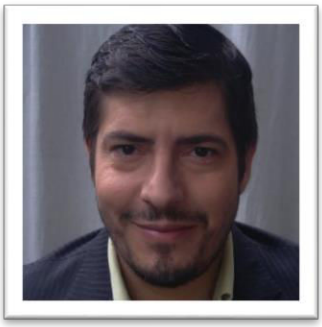
labomarketing
Dopez votre entreprise!

CHECKLIST :
CONFORMITÉ AU R.G.P.D.

Par Didier Bonneville-Roussy & Dushan Jancik

QUI EST DIDIER BONNEVILLE-ROUSSY ?



Didier Bonneville-Roussy est fondateur, président et idéateur de l'autorépondeur Cybermailing. Il fait du marketing internet depuis plus de 20 ans.

Il s'intéresse tout particulièrement aux **leviers technologiques, conceptuels et stratégiques qui vous permettent d'augmenter les résultats de votre entreprise sans augmenter votre investissement en temps, argent et ressources.**

Lorsqu'il n'aide pas ses clients à obtenir plus de résultats de leur marketing, Didier passe son temps avec ses trois garçons, fait du vélo et joue aux échecs... Il habite Montréal, et, au dernier compte, sert des clients dans 82 pays.

QUI EST DUSHAN JANCIK ?

Dushan Jancik est un stratège en Communication, Persuasion et Marketing Internet, depuis 2009.

Il est spécialisé dans la diffusion, la valorisation et la monétisation de l'EXPERTISE. Il est disponible dans certains cas comme consultant, via son site DushanJancik.com...

Il est également le créateur d'un nouveau centre de recherche et formation, le Labo Marketing, dans lequel il partage avec les entrepreneurs francophones **le meilleur des techniques marketing issues de ses propres recherches et de celles des plus grands spécialistes américains.**

REMARQUES PRÉLIMINAIRES

Didier Bonneville-Roussy et Dushan Jancik ne sont PAS des avocats. Ces informations sont fournies sans garanties, et ne sont basées que sur la compréhension actuelle de ces deux entrepreneurs très concernés par les enjeux de la protection des données privées.

Vous êtes bien entendu encouragé à ne prendre cette checklist qu'à titre indicatif, à faire vos propres recherches, et à consulter un avocat spécialisé.

Dernière remarque : cette checklist est basée sur ce que nous croyons être le contexte de la majorité de nos prospects et clients… Elle est loin d'être exhaustive, et il relève de votre responsabilité de vous renseigner sur votre cas particulier.

Par exemple, si le traitement des données relève de votre cœur de métier, si vous traitez des données dites « sensibles » (données médicales, appartenance religieuse, orientation sexuelle, etc.), ou si vous traitez les données de mineurs, alors des cas particuliers s'appliqueront.

Nous espérons que cette checklist, en complément au séminaire d'introduction que nous avons présenté le 3 Mai 2018, vous aidera à y voir plus clair et à mettre en place une méthode de traitement des données plus consciente, efficace, et respectueuse de la vie privée.

Bonne mise en conformité !

Didier & Dushan

LA CHECKLIST R.G.P.D.

1. CONSENTEMENT

- ☐ Avez-vous obtenu un consentement par une action positive sur l'ensemble des données que vous traitez ?
- ☐ Pour les données sur les personnes dont vous n'avez pas obtenu le consentement, avez-vous un plan pour l'obtenir d'ici le 25 mai 2018 ?

  (Le 25 mai 2018, vous ne pourrez plus traiter de données liées aux personnes dont vous n'avez pas la preuve du consentement)
- ☐ Avez-vous informé les personnes dont vous avez obtenu le consentement de leurs droits de retrait, de mise à jour, du droit à l'oubli, du droit à la portabilité et de la possibilité de se retirer du profilage comportemental ?
- ☐ Avez-vous informé les personnes concernées de la durée de validité du consentement ?

  (Vous devez informer les personnes concernées de la durée de ces éléments pour continuer à traiter leurs données.)
- ☐ Avez-vous un plan pour rappeler les droits des personnes concernées régulièrement ?

2. SOUS-TRAITANTS

- ☐ Avez-vous établi la liste de tous vos sous-traitants ?
- ☐ Avez-vous vérifié qu'ils opèrent dans l'U.E. ou dans un

pays au niveau de protection des données adéquat ?

- ☐ Dans le cas contraire, avez-vous vérifié que vos sous-traitants utilisent les clauses contractuelles types de l'U.E. ?
- ☐ Avez-vous vérifié que vos sous-traitants permettent l'exercice des droits suivants « by design » : retrait, oubli, modification, portabilité et non-profilage.
- ☐ Avez-vous vous validé leurs procédures d'information en cas de brèche, vol, perte de données (ils doivent être capables de prévenir dans les 72 heures après le constat) ?
- ☐ Et vous, avez-vous vérifiez que vous êtes capables de prévenir vos clients et la CNIL, dans les 72 heures, en cas de brèche, vol ou perte de donnée ?
- ☐ Avez-vous vérifié si vos sous-traitants ont un représentant dans l'U.E. ?
- ☐ Avez-vous validé l'existence et les coordonnées du Délégué à la protection des données de vos sous-traitants qui le nécessitent ?
- ☐ Votre sous-traitant tient-il un registre des données qu'il traite pour votre compte et le rend-t-ils facilement accessible ?
- ☐ Avez-vous évalué si les mesures de sécurité liées aux données personnelles de vos sous-traitants sont suffisantes ?

3. SÉCURITÉ DES DONNÉES

- ☐ Tous vos formulaires pointent-t-ils vers des liens https ?
- ☐ Vos bases de données sont elle-sécurisées ?

- ☐ Avez-vous établi une procédure de protection des données pour l'ensemble de vos employés et sous-traitants en contacts avez des données personnelles que vous traitez ?
- ☐ Avez-vos établi une politique de gestion de la sécurité des données en interne (mot-de-passes, impressions de fichiers, téléchargement de fichiers, commandes postales et téléphoniques, sécurité des postes de travail, etc.) ?

4. COOPÉRATION AVEC L'AUTORITÉ DE CONTRÔLE

- ☐ Avez-vous nommé un représentant ?
- ☐ Avez-vous établi un registre de données personnelles que vous traitez ?
- ☐ Avez-vous nommé un délégué à la protection des données (DPD), dans les cas où vous en avez besoin ?
- ☐ Avez-vous établi une procédure de rapport d'incident auprès de l'autorité de contrôle et des personnes concernées ?

5. POLITIQUE DE VIE PRIVÉE

- ☐ Avez-vous rédigé une politique de vie privée qui recense l'ensemble de ces informations en un seul document utilisé pour informer clairement et dans un langage simple les personnes concernées sur :
    - Leurs droits
    - Les finalités du traitement

- La durée du consentement
- La procédure d'exercice de leurs droits
- Les sous-traitants et leurs fonctions
- Les transferts de données hors U.E., le pays et le niveau de protection
- Les mesures de sécurité
- Vos coordonnées, celles de votre représentant, celles de votre DPD
- La procédure de rapport d'incident

Lorsque vous avez tout ça, vous êtes normalement conforme, sauf cas particuliers.