RGPD

Les faits

Règlement général sur la protection des données

Le 25 mai 2018, le règlement européen sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Étape 1
Y-a-t'il un pilote dans l'avion ?

INTOX : Obligation de nommer un Délégué à la Protection des Données (ou Data Protection Officer (DPO). Autre obligation pour les entreprises et pas des moindres. Il leur faudra, dès mai 2018, nommer un DPO (data protection officer) ou, en français un DPD (délégué à la protection des données).
Cette obligation s'appliquera à toute autorité publique et à toute entreprise de plus de 250 salariés ou à toute entreprise dont l'activité principale repose sur du traitement de données.

DETOX : Ce délégué à la protection des données est une personne chargée de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par l'organisme.

L'info en plus :

Sa désignation est très fortement conseillée, mais pas obligatoire, sauf pour :

- Les autorités ou organismes publics
- Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle
- Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions

Même si ce n'est pas obligatoire pour votre structure, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », cela vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

Comment devenir délégué ?
https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

le communication MB American Center / agouimenou@monabismarck.org

RGPD

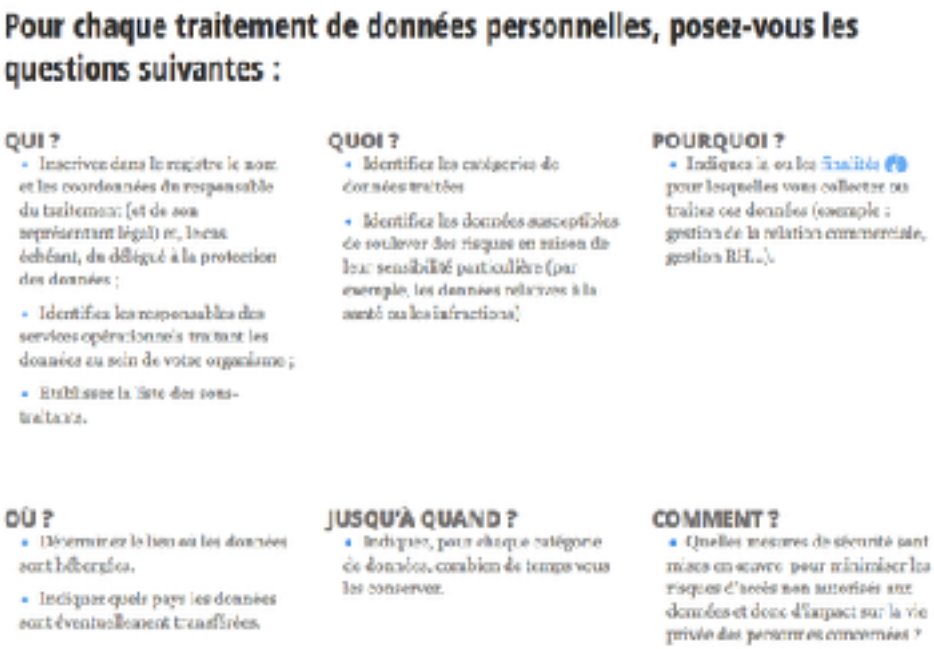
Etape 2 CARTOGRAPHIER

INTOX : Obligation de tenir un registre de l'ensemble des traitements réalisés sur la base.

DETOX
Ce registre ne concerne que les entreprises de plus de 250 salariés, sauf si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernés, s'il n'est pas occasionnel ou s'il porte sur des catégories de données particulières (cf article 9 et 10)**e en œuvre la conformité au règlement européen** sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en
œuvre par l'organisme.

L'info en plus :

"Pour mesurer concrètement l'impact du règlement européen sur la protection des données de votre activité, commencez par recenser de façon précise les traitements de données personnelles que vous mettez en œuvre. La tenue d'un registre des traitements vous permet de faire le point."
Cnil.fr



Audrey Gouimenou - Responsable communication MB American Center /
agouimenou@monabismarck.org

Etape 3
Prioriser les actions à mener

Sur la base du registre des traitements, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

- Assurez-vous que **seules les données strictement nécessaires** à la poursuite de vos objectifs sont collectées et traitées.
- Identifiez **la base juridique** sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)
- Révisez vos **mentions d'information** afin qu'elles soient conformes aux exigences du règlement (articles 12, 13 et 14 du règlement)
- Vérifiez que vos **sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
- Prévoyez les modalités d'exercice des **droits des personnes** concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement…)

Vérifiez les **mesures de sécurité** mises en place

Etape 4
Organiser les processus internes

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire).

DE LA LECTURE…

le livre blanc EUDONET https://goo.gl/ZLto3y
le site Internet de la cnil https://www.cnil.fr/professionnel
Compte rendu de la conférence : http://www.magestionbilletterie.com/2018/02/01/compte-rendu-sitem-2018-rgpd-ce-qui-change-pour-les-professionnels-des-musees-0123/
et l'article du site Desmarais Avocats https://www.desmarais-avocats.fr/acte-1-lue-propose-une-definition-unique-de-la-pseudonymisation/

Audrey Gouimenou - Responsable communication MB American Center /
agouimenou@monabismarck.org

RGPD

F.AQ.
QUELS RISQUES ?

.

En cas de non application du règlement, les sanctions encourues sont :

QUELLES DONNEES ?
- Adresses email
- Numéro de téléphone professionnel (ligne directe) - Fonction ou intitulé de poste
- Adresse postale du lieu de travail, de l'entreprise
Sachez qu'elles font désormais partie intégrante de la liste des donnés personnelles, elles seront donc soumises à la nouvelle règlementation qui empêchera par exemple de recueillir des adresses email via un site tiers ou tout autre moyen non consenti par la personne concernée.

Données de localisation (Adresse IP, Données GPS)
- Cookies «first[1] and third party[2]»
- Numéro d'identification, identifiant
-Eléments correspondants à l'identité physique, psychique, génétique ou économique

Données sensibles
Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

OPT-IN ? CONSENTEMENT ?
Le consentement, dans le cadre de l'email marketing, a longtemps été un sujet ambigu. Le RGPD précise désormais, de façon formelle, que les professionnels du marketing pourront contacter les résidents européens seulement si ces derniers ont donné en amont un consentement explicite. En d'autres termes, cela marque la fin des envois d'emails non sollicités en BtoC. Néanmoins, le règlement reste flou concernant le BtoB. Il est fort probable qu'à termes le BtoB soit considéré comme le BtoC.

Audrey Gouimenou - Responsable communication MB American Center /
agouimenou@monabismarck.org

RGPD

PAR OÙ JE COMMENCE ?

Provenance du contact

Ajouter la provenance du contact (intermédiaire par lequel il a été récupéré : newsletter, livre blanc, webinaire, salon, application mobile...). Dans les bases de données marketing, (CRM ou Datamart), un champ devra être également ajouté concernant la date de création du contact et ce, dans toutes les bases de données.

Exportation des données

S'assurer qu'il est possible d'exporter l'ensemble des données concernant un ou plusieurs clients en cas de contrôle par les autorités ou sous la demande explicite d'un client. Par exemple, depuis votre outil de gestion de campagnes emailing, il faut pouvoir exporter les données et y intégrer les deux éléments cités ci-dessus (provenance et date d'acquisition).

Les mentions légales

Réécrire les mentions légales du site internet comportant les nouvelles mentions obligatoires comme la nature des données collectées et leurs finalités. (Votre âge est nécessaire car les produits commercialisés ne conviennent pas aux mineurs). Doit y figurer également le délai de conservation des données

Synchroniser le site internet avec les bases de données enrichies par les formulaires en opt-in pour pouvoir déclencher des campagnes marketing en opt-in.

Les formulaires

Mettre à jour les formulaires avec l'ajout de cases à cocher, et des mentions claires afin que les internautes donnent leur accord ou non pour chaque utilisation de données (email, revente de données à un tiers...)

Données automatisées

Mettre en place une suppression des données automatisée pour les contacts inactifs depuis plus de trois ans.

Cookies explicites

Faire évoluer des bandeaux de cookies afin qu'ils soient plus explicites et que leur durée de vie soit de treize mois maximum. Passé ce délai, le consentement de l'internaute devra être à nouveau recueilli.

Audrey Gouimenou - Responsable communication MB American Center /
agouimenou@monabismarck.org

Audrey Gouimenou - Responsable communication MB American Center /
agouimenou@monabismarck.org