RGPD

GROUPE ACCOR
Sanction de 600 000€
Défaut de consentement
Mots de passe insuffisamment robustes
...etc.

UBEEQO
Sanction de 175 000€
Collecte de données de géolocalisation permanente non justifiée
Durées de conservation non définies et non respectées
...etc.

DEDALUS BIOLOGIE
Sanction de 1 150 000€
Non encadrement juridique de la sous-traitance de données
Manquement à la sécurité des données
...etc.

CYBERSECURITE

Un Ehpad de Normandie victime d'une cyberattaque, le plan blanc déclenché.

L'hôpital sud francilien de Corbeil Essonne a été victime d'une cyberattaque bloquant son système informatique.

L'Union nationale d'aide du Calvados, entreprise sociale de services à la personne et à domicile, a subi une importante cyberattaque dont elle s'est rendue compte le 15 août 2022. Les logiciels de l'association se sont avérés inexploitables

L'ASTUCE

Gestion des mots de passe

Pour qu'un mot de passe soit sécurisé, nous vous recommandons d'utiliser des Majuscules, Minuscules, Caractères spéciaux, Alphanumérique et 12 caractères minimum. Votre mot de passe doit être systématiquement différent selon le service auquel vous accédez.

Pour simplifier la gestion de ces mots de passe, vous pouvez utiliser un outil tel que Keepass (recommandé par l'ANSSI).

Pour cela suivez le lien :
https://keepass.info/download.html

AVIS D'EXPERTS :
Prospection associative et partage d'informations

Rappel des principes inhérents au traitement de données à caractère personnel
Les bases juridiques sur lesquelles un traitement de données à caractère personnel non sensibles peut reposer sont détaillées à l'article 6 du RGPD. En tant qu'association, les principales bases juridiques sur lesquelles vous pourrez vous reposer sont :

- Le consentement de la personne
- Un contrat
- Une obligation légale
- Votre intérêt légitime tout en respectant les droits et libertés des personnes concernées

Concernant les données à caractère personnel sensibles, les conditions sont différentes et sont énoncées à l'article 9 paragraphe 1 du RGPD. De manière générale, un tel traitement ne pourra reposer que sur :

- Le consentement de la personne
- Une obligation en tant que responsable de traitement au regard du droit du travail, de la sécurité sociale et de la protection sociale, sous réserve que le droit européen, le droit national ou votre convention collective l'autorise
- Votre activité légitime, à condition que votre association poursuive une finalité politique, philosophique, religieuse ou syndicale et que les traitements ne concernent que des membres et anciens membres et que les données à caractère personnel ne soient pas communiquées en externe.

Ainsi, afin de pouvoir réaliser de la prospection et/ou partager des informations entre associations, il sera nécessaire que la collecte initiale des données repose sur un fondement licite. Dans le cadre de la prospection, d'autres règles spécifiques sont à respecter.
La prospection associative
Il est ici important d'identifier la nature des différentes actions de prospection que vous menez et plus particulièrement si celles-ci revêtent un caractère commercial ou non. En effet, les règles applicables seront différentes selon la nature retenue.
S'agissant de la prospection commerciale, vous devrez recueillir le consentement actif de la personne concernée sauf si celle-ci est déjà membre de l'association ou a déjà été « cliente » de l'association. Le cas échéant, vous aurez la possibilité de la solliciter pour des produits ou services similaires sans avoir à recueillir son consentement.
Toutefois, la majeure partie des actions de prospection d'une association est de nature non commerciale. Dans ce cas précis, le consentement de la personne ne sera pas nécessaire. Il faudra néanmoins informer la personne sur ce traitement et lui permettre de s'y opposer facilement à l'aide d'une case à cocher.
La mise en place d'un partage d'informations entre associations
La prospection non commerciale et le partage d'informations sont des traitements bien souvent connexes au sein des associations. Afin de pouvoir partager des informations, les associations devront respecter les recommandations énoncées ci-dessous.
Un partage vers des associations poursuivant le même objet
Une condition fondamentale au partage d'information est que les associations avec lesquelles les données sont partagées poursuivent un même objet que l'association à l'origine de la collecte de données.
Une information claire des personnes
Lors de la collecte de leurs informations, les personnes doivent être informées de manière distincte que :

- Leurs données seront utilisées par le responsable de traitement à des fins de prospection caritative
- Leurs données sont susceptibles d'être transmises à d'autres entités uniquement à des fins identiques.

Il faudra d'ailleurs communiquer aux personnes concernées la liste des entités en question. Nous vous recommandons d'intégrer dans les mentions d'information un lien menant à cette liste.
Prêtez également attention à la « quantité » de données partagées sur une même personne. En effet, seules les données strictement nécessaires à la poursuite de la finalité doivent être collectées puis, en l'absence d'opposition, partagées.
Un droit d'opposition distinct
Les mentions d'information évoquées ci-dessus devront préciser que les personnes ont la possibilité de s'opposer séparément à la prospection ou au partage de leurs informations, ou aux deux finalités simultanément.
Il est également recommandé de mettre en place un droit d'opposition distinct pour chacune des associations avec lesquelles un partage d'informations pourrait être réalisé.
Cependant, l'application de ce droit d'opposition (opt out) n'est possible que pour le partage de données à caractère personnel courantes. S'agissant des données à caractère personnel sensibles vous n'aurez pas la possibilité de les partager en l'absence du consentement actif de l'utilisateur.
Informer les entités destinataires des données
Les entités destinataires devront être informées que celles-ci ont l'obligation d'informer les personnes concernées, au plus tard 30 jours après la mise en œuvre d'un traitement sur les données communiquées, la source des données et leur permettre de s'opposer à tout moment à ce traitement.
A cet effet, il est conseillé de mettre en place un avenant RGPD venant encadrer ce partage et la responsabilité entre ces entités et l'association à l'origine de la collecte et du partage.
La mise en conformité a posteriori du partage d'informations
Pour toute association ayant déjà mis en place ce partage de données à caractère personnel, pas de panique ! Il est toujours possible de mettre en conformité le traitement a posteriori, à condition de l'interrompre jusqu'à ce que celui-ci le soit. Vous devrez alors contacter l'ensemble des personnes dont les données ont été partagées, les informer de manière exhaustive sur les différents partages effectués et leur laisser un délai de 30 jours afin de leur permettre d'exprimer leur opposition à ce partage.

Nos Actualités Septembre 2022

Lancement de deux nouvelles offres

Check-up Protection des données

Un questionnaire, une analyse par nos services et un debriefing par un délégué à la protection des données.

Consultation d'expert

1H00 de consultation avec un de nos experts sur le thème de votre choix.

Partenariat formation CFA de BLAGNAC

myDigitplace intervient dans le cadre de la formation des
BTS SIO
et
BACHELOR AIS.

Les objectifs sont de les former à la réglementation informatique et au Hacking Éthique.

Vous recherchez un alternant, contactez-nous : (contact@mydigitplace.com)

Accueil de 2 nouvelles collaboratrices

Nous accueillons **:**

Rim ROUDIES
et
Bahia FALENTIN

Au sein de notre équipe de juristes, elles auront pour mission d'appuyer en renfort nos délégués à la protection des données.

Nous leur souhaitons la bienvenue