Le RGPD au quotidien chez Meubles Tavelot

Meubles Tavelot, magasin de meubles et de décoration de 15 salariés installé à Orange (Vaucluse), vend en magasin et sur son site marchand, et livre dans tout le Vaucluse et la Drôme. Tom Vergier, chargé de la relation client à distance, met en conformité la collecte, l'organisation et la sécurité des données clients.

Pour chaque situation, choisissez la bonne réponse.

Lors d'une commande en ligne, le site enregistre l'adresse de livraison, le téléphone du client et le contenu de la commande. Quelle est la base légale de ce traitement ?

☐ L'intérêt légitime de l'entreprise (le suivi des livraisons)
☐ L'exécution du contrat (la vente et la livraison)
☐ Le consentement du client (case cochée lors de la commande)

Justification :

Le formulaire d'inscription à la lettre d'information exige le nom, le prénom, l'e-mail, la date de naissance, la profession et la situation familiale. Que faut-il en penser ?

☐ C'est conforme, à condition d'indiquer dans la mention d'information du formulaire à quoi servent la date de naissance, la profession et la situation familiale de l'abonné
☐ C'est conforme : connaître le prénom, l'âge, la profession et la famille de l'abonné permet de personnaliser la lettre et de mieux cibler les offres
☐ Il ne faut demander que les données nécessaires à l'envoi de la lettre : l'e-mail, éventuellement le prénom pour personnaliser ; les autres champs sont à retirer

Justification :

La mention d'information placée sous le formulaire de demande de devis doit indiquer : (plusieurs réponses)

☐ L'identité de Meubles Tavelot, qui collecte les données
☐ Le numéro de déclaration du fichier auprès de la CNIL
☐ La durée de conservation des données et les droits de la personne
☐ La finalité : pourquoi les données sont collectées

Justification :

Pour envoyer des offres par SMS aux particuliers qui demandent un devis, le développeur propose d'ajouter au formulaire une case déjà cochée « J'accepte de recevoir les offres par SMS ». Que lui répondre ?

☐ La case doit être non précochée : le consentement suppose une action positive de la personne, et l'entreprise en conserve la preuve
☐ La case peut rester précochée : le client qui ne veut pas des offres la décoche lui-même, et l'entreprise conserve la trace de son choix
☐ La case peut rester précochée : chaque SMS proposera de se désinscrire en répondant STOP, ce qui vaut consentement de la personne

Justification :

M. Chaix, client depuis 2024, demande l'effacement de toutes ses données, y compris ses factures. Que doit faire Tom ?

☐ Effacer les données utilisées pour la prospection et la fidélisation, conserver les factures en archive (obligation légale de 10 ans) et lui répondre dans le mois en expliquant pourquoi
☐ Refuser la suppression tant que M. Chaix reste client : ses données, factures comprises, sont conservées 10 ans à compter de son dernier achat, puis effacées
☐ Effacer l'ensemble de ses données, factures comprises, et lui confirmer l'effacement dans le mois, car le droit à l'effacement l'emporte sur l'obligation d'archivage

Justification :

Meubles Tavelot confie l'envoi de sa lettre d'information à une plateforme d'e-mailing. Que doit-elle faire ?

☐ Recueillir à nouveau le consentement de chaque abonné, puisque ses données passent à une autre entreprise, puis envoyer le fichier à la plateforme chaque mois par e-mail
☐ Lui transférer la responsabilité du fichier par contrat : devenue responsable de traitement, la plateforme répond désormais à la place de Meubles Tavelot des données de ses clients
☐ Signer avec la plateforme un contrat qui fixe ses obligations de protection des données, et vérifier où les données sont hébergées, de préférence dans l'Union européenne

Justification :

Lesquelles de ces pratiques protègent le fichier clients ? (plusieurs réponses)

☐ Activer la double authentification sur le CRM
☐ Copier le fichier sur une clé USB personnelle pour travailler chez soi
☐ Supprimer le compte CRM d'une vendeuse le jour de son départ
☐ Envoyer la liste des livraisons au transporteur en pièce jointe non protégée

Justification :

Une vendeuse a saisi son mot de passe du CRM sur une fausse page de connexion reçue par e-mail. Quelle est la bonne réaction ?

☐ Supprimer l'e-mail frauduleux et garder le même mot de passe, puis prévenir le délégué à la protection des données lors du prochain point mensuel, qui notifiera la CNIL dans le délai d'un mois si des clients se plaignent
☐ Changer aussitôt le mot de passe, prévenir le référent ou le délégué à la protection des données et suivre la procédure d'incident : si des données clients ont été consultées et que cela présente un risque pour eux, notifier la violation à la CNIL sous 72 heures
☐ Changer son mot de passe à la prochaine connexion sans alerter personne, puisque les fiches du CRM sont intactes : une violation ne se notifie à la CNIL que si des données ont disparu ou ont été modifiées

Justification :

Le bandeau cookies du site affiche un grand bouton vert « Tout accepter » et, en petit, un lien gris « Paramétrer ». Est-il conforme ?

☐ Oui : le lien « Paramétrer » permet à l'internaute de refuser les traceurs, et le bouton vert de les accepter, ce qui lui laisse le choix
☐ Non : refuser doit être aussi simple qu'accepter, par exemple avec un bouton « Tout refuser » de même présentation
☐ Oui, si les traceurs ne sont déposés qu'après 30 secondes de navigation, la poursuite de la navigation valant accord de l'internaute

Justification :