

Newsletter

DATA



Protection des données personnelles et envoi d'un message WhatsApp à des fins personnelles

RGPD / WhatsApp / Détournement de finalité

SYNTHÈSE - Par décision du 25 août 2020, l'Autorité de protection des données espagnole a sanctionné un travailleur indépendant pour avoir contacté une cliente via WhatsApp.

FAITS - Un travailleur indépendant avait été missionné par une entreprise afin qu'il réalise des travaux de plomberie au domicile de la plaignante. Lors de la visite du plombier, celle-ci lui avait fourni son numéro de téléphone dans le but de gérer les travaux et leur éventuel suivi.

Séduit par sa cliente, le plombier a envoyé un message WhatsApp à cette dernière, à des fins de lui faire des avances.

Or, initialement, le numéro de téléphone de la cliente avait été collecté pour la bonne réalisation et le suivi des travaux de plomberie.

Pour cette raison, la cliente a saisi l'Autorité espagnole de protection des données afin de se plaindre dudit message et de l'utilisation de son numéro de téléphone portable à des fins autres que la gestion et le suivi des travaux de plomberie.

SOMMAIRE

Protection des données personnelles et envoi d'un message WhatsApp à des fins personnelles 1

Protection des données personnelles et messagerie électronique sur le lieu de travail : que peut-on faire du compte du collaborateur sortant ? 2

Messagerie électronique sur le lieu de travail : l'autorité de protection des données belge précise les mesures à mettre en œuvre lors du départ d'un salarié 2

Consentement et cookies : la CNIL fournit ses recommandations pratiques 3

L'une des rares amendes infligées jusqu'à présent aux sous-traitants de données dans le cadre du RGPD a été récemment prononcée par l'autorité de contrôle italienne 4



Validant le raisonnement soutenu par la cliente, l'Autorité espagnole a considéré que le travailleur indépendant avait violé le principe de limitation des finalités posé par l'article 5 (1) (b) du RGPD, en utilisant le numéro de téléphone de la cliente pour des fins auxquelles celle-ci n'avait pas consenti.

SANCTION - Une amende administrative de 2 000 euros a alors été imposée au travailleur indépendant qui avait utilisé WhatsApp à mauvais escient.

DÉCISION – [Cliquez ici pour en savoir plus](#) (AEPD, Procedimiento N°: PS/00383/2019, 25 août 2020)

Protection des données personnelles et messagerie électronique sur le lieu de travail : que peut-on faire du compte du collaborateur sortant ?

RGPD / Italie / Salarié / Messagerie électronique

SYNTHÈSE - Dans une décision rendue le 2 juillet 2020, l'Autorité de protection des données italienne a statué sur la question de la suppression d'un compte de messagerie électronique professionnelle d'un salarié après la rupture de sa relation de travail avec son employeur.

FAITS - L'ancien employé d'une entreprise spécialisée dans le secteur de la construction a réalisé que son employeur avait maintenu ouvert et fonctionnel son compte de messagerie électronique après la fin de la relation de travail qui les liait. Un transfert automatique de l'ensemble des messages entrants avait été mis en œuvre, vers la messagerie de son supérieur hiérarchique. Cette action, comme souvent, visait simplement à permettre la continuité des opérations de l'entreprise.

Saisie par l'ancien collaborateur, dans sa décision, l'Autorité italienne sanctionne l'employeur pour plusieurs motifs :

- D'une part, elle estime que la durée pendant laquelle le compte a été maintenu

après le départ du collaborateur est longue : un peu plus de 10 mois, et notamment, en violation du secret des correspondances.

- D'autre part, elle considère que l'employeur n'avait pas fourni aux employés d'informations quant à la règle de transfert automatique mise en œuvre sur la messagerie des collaborateurs sortants, en violation du droit à l'information de toute personne concernée.

L'Autorité italienne considère que l'employeur aurait dû adopter des mesures techniques et organisationnelles adaptées pour permettre le maintien de l'activité opérationnelle de l'entreprise, tout en garantissant la protection des données personnelles du collaborateur sortant. Par ailleurs, elle renforce la règle selon laquelle il est nécessaire de préciser dans la documentation fournie aux employés quel sera le sort de leur compte de messagerie professionnelle après leur départ de l'entreprise.

SANCTION - L'Autorité italienne a sanctionné l'employeur à une amende administrative de 15 000 euros.

DÉCISION – [Cliquez ici pour en savoir plus](#) (Garante per la protezione dei dati personali, n° 115, 2 juillet 2020)

Messagerie électronique sur le lieu de travail : l'autorité de protection des données belge précise les mesures à mettre en œuvre lors du départ d'un salarié

RGPD / Belge / Salarié / Messagerie électronique

SYNTHÈSE - Dans une décision rendue le 29 septembre 2020, l'Autorité de protection des données belge a eu l'occasion de préciser les mesures à mettre en œuvre concernant la messagerie professionnelle d'un salarié, lors du départ de celui-ci.

FAITS - Le responsable de traitement (une petite entreprise employant une dizaine de



salariés et agissant dans le secteur des dispositifs médicaux) avait fait l'objet d'une plainte d'un ancien salarié mécontent. Lorsqu'il était en fonction, ce dernier avait eu un rôle d'administrateur délégué de l'entreprise. Il avait sollicité auprès de la défenderesse de cesser toute utilisation de 7 adresses emails (et de clôturer les comptes associés) qui lui étaient liées ou qui utilisaient le nom et le prénom d'un membre de sa famille. Il estimait, en outre, que les échanges contenus dans ces comptes étaient protégés par le secret des correspondances et qu'ils contenaient des données protégées par le secret médical. Enfin, il se plaignait du fait que tous messages entrants ou sortants faisaient l'objet d'un renvoi vers l'adresse email d'un autre salarié de l'entreprise.

Dans ce contexte, l'autorité belge a clairement affirmé que :

- En application des principes de finalité, de minimisation et de conservation limitée, le responsable de traitement doit bloquer la messagerie électronique professionnelle de l'employé sortant au plus tard le jour du départ effectif de celui-ci.
- Ce blocage devra intervenir après l'en avoir averti au préalable et après y avoir fait insérer un message automatique avertissant tout correspondant ultérieur du fait que la personne concernée n'exerce plus ses fonctions au sein de l'entreprise. Le message automatique doit également faire mention des coordonnées de la personne (ou l'adresse email générique) à contacter, pendant une période de temps raisonnable. En principe, ce délai doit être fixé à un mois. Il pourra être étendu à trois mois si cela est justifié par les fonctions de l'employé sortant, après avoir obtenu l'autorisation de celui-ci, ou, à tout le moins, après l'en avoir averti.
- A l'issue de ce délai, le compte et l'adresse email associée doivent être supprimés.
- En tout état de cause, il convient d'éviter un transfert automatique des courriers entrants et sortants vers une autre

messagerie électronique. Cela pose un risque significatif pour l'employé sortant mais également pour le correspondant pensant communiquer avec ce dernier.

SANCTION - N'ayant pas respecté ces étapes dans sa procédure de sortie des employés, le responsable de traitement a été sanctionné d'une amende administrative de 15 000 euros par l'autorité belge de protection des données.

DÉCISION - [Cliquez ici pour en savoir plus](#) (Chambre contentieuse, *Décision quant au fond 64/2020 du 29 septembre 2020*)

Consentement et cookies : la CNIL fournit ses recommandations pratiques

[Cookie / Traceurs / France / CNIL](#)

SYNTHÈSE - La CNIL a fourni des recommandations pratiques complétant ses lignes directrices relatives aux cookies et autres traceurs. Celles-ci visent à préciser les modalités pratiques à mettre en œuvre pour collecter valablement le consentement des utilisateurs.

En principe, sans consentement, aucun traceur ne peut être lu ou déposé sur le terminal de l'utilisateur (sauf rares exemptions prévues par la Loi Informatique et Libertés). Mais encore faut-il que ce consentement puisse être considéré, juridiquement, comme valide !

A ce titre, pour être valide, il est rappelé que le consentement soit libre, spécifique, informé et non équivoque.

FAITS - Selon la CNIL, pour qu'un consentement remplisse ces critères, il doit :

- Résulter d'un acte positif clair : l'inaction de l'utilisateur, sa visite sur d'autres pages du site ou le fait qu'il scrolle la page d'accueil ne permettent pas de considérer qu'il s'agit d'un acte clair et positif.
- Être fourni après que l'utilisateur ait été informé des finalités des cookies et traceurs et des responsables de traitements (conjointes ou disjointes). Il



convient de fournir une liste exhaustive de ces derniers, accessible dans une version toujours mise à jour pour l'utilisateur.

- Résulter d'un acte non équivoque : les cases pré-cochées ou les sliders en mode « on » sont à proscrire.
- Etre fourni librement : il doit être possible de fournir un consentement par finalité. En plus, des boutons « tout accepter » ou « tout rejeter » doivent être prévus. Les cookies walls, bien que non recommandés, ne sont pas interdits.

Par ailleurs, il est recommandé de mettre en œuvre les modalités pratiques suivantes :

- Le consentement doit être renouvelé après un laps de temps approprié (par exemple, tous les 6 mois).
- La bannière « cookies », ou pop-up, doit être supprimée si l'utilisateur n'effectue aucune action dessus, après un court laps de temps, pour éviter de gêner son usage.
- Enfin, il doit être possible de retirer le consentement aussi facilement qu'il a été donné. Les utilisateurs doivent être informés à tout moment des méthodes à leur disposition pour retirer leur consentement : par exemple, une icône « cookie » peut être incluse sur chaque page du site Internet afin que l'utilisateur puisse accéder à ses préférences directement, à tout moment. Cela peut également être effectué par le biais d'un lien hypertexte disponible sur toutes les pages du site Internet.

Enfin, il est rappelé que ces recommandations s'appliquent à tout site Internet, toute application mobile, tout objet connecté, console de jeux, assistant vocal, c'est-à-dire, à tout applicatif permettant de déposer ou de lire des cookies ou traceurs sur le terminal d'un utilisateur, qu'ils traitent, ou non, des données personnelles.

DÉCISION – [Cliquez ici pour en savoir plus](#) (Délibération n° 2020-092, du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en

conformité en cas de recours aux « cookies et autres traceurs »)

L'une des rares amendes infligées jusqu'à présent aux sous-traitants de données dans le cadre du RGPD a été récemment prononcée par l'autorité de contrôle italienne

RGPD/Italie/ST/Sanction

SYNTHÈSE - L'Autorité de protection des données italienne a eu l'occasion de sanctionner un sous-traitant en application du RGPD.

FAITS - Le responsable de traitement, l'Azienda Ospedaliera (un hôpital privé), organisait un concours public et avait confié à Scanshare s.r.l., un sous-traitant informatique, le service de gestion des candidatures en ligne et la phase de présélection informatique des candidats.

En raison d'une erreur de configuration, une liste de codes attribués aux candidats était temporairement accessible sur Internet, via un lien « http://... ». Par ce biais, il était possible d'accéder aux documents soumis par les candidats, contenant leurs données personnelles, dont certaines données sensibles (données de santé). En insérant le matricule du candidat dans un champ donné, il était même possible de modifier les documents et données insérées par les candidats.

Dans ce contexte, l'Autorité italienne a sanctionné le prestataire informatique Scanshare s.r.l. en se fondant sur plusieurs éléments, notamment :

- Le défaut de mise en place de mesures de sécurité suffisante, de la collecte au traitement des données des candidats. Par exemple, la collecte pouvait être effectuée via l'envoi d'un CD sans chiffrement ou mot de passe
- La poursuite du traitement des données des candidats au jour de la sanction rendue par l'autorité italienne, alors que toute relation contractuelle avec le responsable de traitement avait cessé.



SANCTION - L'amende infligée au sous-traitant pour violation des articles 5 (1) a), 6, 9 et 32 du GDPR s'élève à 60 000 euros.

DÉCISION – [Cliquez ici pour en savoir plus](#)
(*Garante per la protezione dei dati personali, provvedimento n° 161, 17 settembre 2020*)