UNDIA
ASSOCIATION FRANÇAISE
RÉGIE PAR LA LOI DU
1ER JUILLET 1901
UNDIA
35 bd de Bonne-Nouvelle
75002 Paris
undia@undia.fr
www.undia.fr
UNION NATIONALE DE DÉFENSE DES INTERMITTENTS DE L'AUDIOVISUEL

UNDIA et vos données

UNDIA LE 25 MAI 2018

Pourquoi ?

Dans le cadre du nouveau règlement n°2016/679, dit Règlement Général sur la Protection des Données (ci-après nommé RGPD), UNDIA a décidé d'exposer les pratiques de l'association, et les règles qu'elle applique depuis sa naissance en juillet 2017. Nous n'avons pas attendu le RGPD pour opter pour des règles très strictes, mais nous n'avions pas communiqué à ce sujet. C'est chose faite désormais avec cette déclaration qui nous engage vis-à-vis de vous.

Le RGPD entre en vigueur dans l'Union Européenne le 25 mai 2018. Dès lors qu'il vise de quelque manière que ce soit les citoyens d'un État membre, tout service qui traite des données informatiques doit se conformer à ce règlement.

Le site www.undia.fr et l'UNDIApp entrent dans ce cadre. Nous vous expliquons quelles sont les données que nous recueillons chez UNDIA, pourquoi et comment nous les gérons, quels sont nos engagements vis-à-vis de la confidentialité, et quels sont vos droits.

La collecte de données

UNDIA collecte un certain nombre de renseignements à caractère personnel dès votre inscription comme UNDIAmi ou comme adhérent UNDIA.

UNDIAmis

Ces renseignements sont, en ce qui concerne nos UNDIAmis, les genre, nom, prénom, date de naissance, surnom, adresse courriel et les professions intermittentes exercées de la personne qui s'inscrit. La base contient également le mot de passe chiffré selon la méthode la plus sécurisée utilisée par l'industrie web actuelle, ainsi que divers réglages de préférences de l'UNDIAmi, date de son inscription et de ses récentes connexions, sur le site et l'UNDIApp.

L'ensemble de ces données permettent d'envoyer des informations mieux ciblées aux personnes qui les reçoivent. Ceci évite la surcharge en courriels, par exemple en envoyant seulement aux personnes de la post-production un renseignement concernant la post-production et seulement la post-production. Ces informations permettent également à l'UNDIAmi de s'assurer qu'il ne s'est pas fait voler ses informations de connexion, et le cas échéant, de les changer.

Ils permettent également de distinguer les doublons dans notre base de données, de faire la différence entre deux homonymes (même nom, même prénom), et plus généralement de mieux servir ceux qui y sont inscrit, évitant les envois de courriels en double.

Enfin, il nous donnent une image de qui sont les intermittents de l'audiovisuel, ce qui nous permet d'expliquer aux institutions que nous rencontrons et avec qui nous traitons, qui ils sont et ce qu'ils font.

Adhérents

La fiche remplie lors de l'adhésion est une fiche standard d'adhésion en association. Elle compte la fiche UNDIAmi (genre, nom, prénom, surnom, date de naissance, adresse courriel et professions), ainsi qu'une adresse postale, un numéro de mobile et stocke également quelques préférences de l'adhérent par rapport au site. Elle stocke également la date de début de l'adhésion, de fin d'adhésion, le nombre d'année d'adhésion ainsi que l'historique d'adhésion.

L'adhérent a par ailleurs la possibilité, s'il le souhaite, de renseigner son expérience professionnelle sur le site, ainsi que ses compétences. Ces informations ainsi que le numéro de mobile seront utilisées dans le cadre de l'expérimentation d'un forum métier qui mettra à terme en relation les intermittents et les productions.

Le numéro de mobile permet par ailleurs, dans certains cas, de contacter l'adhérent si son adresse courriel vient à ne plus fonctionner ou à changer, et permet de s'assurer donc que l'adhésion n'est pas « volée » par une tierce personne.

L'UNDIApp

L'UNDIApp est application pour téléphone qui aide à calculer et suivre sa vie intermittente. Elle contient des données sensibles de revenus de l'intermittent qui l'utilise. Ces données ne quittent jamais le téléphone de la personne concernée. UNDIA garanti le caractère local du stockage des données de revenus.

L'UNDIApp communique avec le site pour vérifier que l'utilisateur est bien un UNDIAmi inscrit sur le site, ainsi que pour télécharger les nouvelles de l'association et les liens utiles. Seules certaines données de base UNDIAmi et adhérent de l'utilisateur identifiés pourront être consultées depuis l'UNDIApp.

Nous avons décidé de concevoir comme telle l'UNDIApp pour la rendre intrinsèquement sûre. Le temps consacré à la fabrication de cette App par UNDIA la destine à notre communauté, nous demandons donc aux utilisateurs d'en faire partie avant de pouvoir l'utiliser.

En conséquence de ce qui précède, les données de revenus contenues dans l'App ne sont pas sous la responsabilité d'UNDIA, mais uniquement celle de l'utilisateur, qui est donc tenu de sauvegarder ces données, et de protéger l'accès à son téléphone. Afin qu'elles ne soient pas dérobées par des tiers qui auraient physiquement accès à l'appareil (perte, vol), l'utilisateur se doit d'être proactif en matière de sécurité, notamment mais pas uniquement en utilisant un code fort de verrouillage (6 chiffres minimum) et l'effacement automatique en cas de tentatives d'accès non autorisées.

En aucun cas UNDIA ne saurait être tenu responsable de fuite de données locale sur un appareil d'un utilisateur.

La plateforme OneSignal

Afin d'envoyer des notifications aux utilisateur de l'UNDIApp, nous utilisons un service tiers nommé OneSignal. Cette plateforme d'envoi de notifications reçoit de notre part :

- un identifiant créé spécifiquement qui anonymise l'utilisateur ;
- le modèle de l'appareil, version de système d'exploitation et de l'UNDIApp, nécessaires pour que la notification puisse être comprise par l'appareil qui la recevra ;
- le type d'utilisateur (adhérent ou membre ayant des fonctions spécifiques dans l'association) ;
- la dernière utilisation pour rappeler à l'utilisateur de ne pas oublier de compléter son dossier.

Aucune de ces informations, seule ou agrégée aux autres, ne permet d'identifier l'utilisateur. OneSignal ne reçoit donc, stricto sensu, aucune donnée à caractère personnel.

Les paiements en ligne

Les paiements en ligne sont effectués techniquement par notre banque. La banque nous communique seulement le résultat du paiement. Elle nous envoie également quelques informations qui permettent de retrouver les paiements dans la base de données et lutter contre les fraudes ou tentatives de fraudes à la carte bancaire.

Ces informations sont :

- un identifiant irréversible de la carte, c'est à dire qu'il est mathématiquement impossible d'en retrouver le numéro ;
- la date de validité, le pays d'émission et le réseau de la carte ;
- le résultat positif ou négatif des tests de sécurité effectués (3DSecure, crypto), mais en aucun cas les informations des tests elle-même ;
- le numéro de la transaction et le numéro de la banque débitrice ;
- l'ip et le pays de l'ip de la personne qui a effectué la transaction.

Les informations fournies par la banque ne permettent pas d'identifier nominativement le payeur, et ne permettent absolument pas de faire ou refaire un paiement. C'est la raison pour laquelle les adhérents devront payer chaque année manuellement leur cotisation.

Ces informations sont regroupées dans une base nommée bande journal qui permet à notre trésorier et notre vice trésorier de suivre l'activité bancaire, et repérer des irrégularités le cas échéant. Ils sont les seuls à y accéder.

Le traitement des données

La base contenant les données de toutes les personnes qui sont inscrites d'une manière ou d'une autre sur UNDIA est une base fermée dont l'accès est uniquement limité aux personnes gérant le site web. Ce groupe est volontairement constitué d'un nombre très restreint de personnes (1 à 2 maximum).

Il est par ailleurs impossible à tous les autres utilisateurs (bureau et CA compris) d'accéder à l'intégralité de la base. Cette pratique permet d'éviter qu'une personne ayant un accès en raison de sa fonction particulière dans l'association, et qui se serait fait voler son mot de passe, devienne à son corps défendant le moyen pour des personnes ou des organismes mal intentionnés d'accéder à la base elle-même.

Les outils de gestion de la base brute, contenant toutes les données, sont protégés par notre hébergeur, qui exclue toute connexion directe à la base de donnée, et qui se ferait depuis l'extérieur du site undia.fr : la consultation des données doit passer obligatoirement par le site lui même, ou bien par l'interface de notre hébergeur. Celle-ci est protégée par une authentification à deux facteurs dont l'accès n'est possible qu'à une seule personne. Les bases de données sont protégées par des mots de passe très forts changés régulièrement.

Les accès aux données et au traitement de celles ci dépendent des fonctions dans l'association.

L'UNDIAmi et l'adhérent

Ces derniers peuvent accéder dans leur espace personnel à leurs données personnelles et uniquement celles-ci. Le site est conçu pour leur refuser l'accès à celles des autres personnes.

L'UNDIAmi ou l'adhérent peut choisir d'être joignable via le site, il peut alors être retrouvé sur le site. Dans ce cas un demandeur va le rechercher sur le site. Un sas entre les deux parties est mis en place (aucune information n'est communiquée au demandeur), jusqu'à ce qu'elles aient librement décidé d'entrer en contact. La transmission des infos de contact au demandeur est du seul ressort et de la seule décision de la personne qui a été contactée. Le site limite à une certaine quantité ces demandes par jour et par personne afin d'empêcher par contrainte de temps le vol de données.

Les informations que l'UNDIAmi ou l'adhérent a choisi de rendre publiques le sont jusqu'à ce qu'il ait décidé le contraire, et seules les informations pour lesquelles ceci a été choisi le sont.

Le bureau et le CA

Le bureau et le CA, selon les fonctions qui le composent, ont accès à un certain nombre de données supplémentaires, notamment statistiques. Il peuvent voir des chiffrages généraux à propos de la base des UNDIAmis (et donc des adhérents).

En revanche, aucun membre du bureau ou du CA ne peut télécharger de listing, et s'ils ont accès à une liste, elle est volontairement réduite aux renseignements indispensables permettant de retrouver quelqu'un. Cette façon de faire évite l'aspiration de liste par des personnes ou des organismes malveillants via un accès volé, mais authentique. Les membres du bureau et du CA peuvent rechercher dans la base des noms mais sont limité à un certain nombre de résultats, et sont donc contraints de préciser leur critères. Cette

pratique évite que des recherches vagues permettent des accès à de larges quantités de données.

Les membres du bureau concernés par la trésorerie ont accès à des informations financières (règlements de cotisation, reçus de carte), qui leur sont exclusivement réservées. Ces membres sont le trésorier et le vice-trésorier. Les autres membres du bureau peuvent voir des informations partielles et générales, qui concernent les finances de l'association dans leur globalité, mais en aucun cas des détails contenant des informations personnelles.

Toute publication financière de l'association est par ailleurs purgée des informations personnelles et spécifiques qu'elle pourrait contenir, pour ne s'intéresser qu'au bilan général. Ces publications sont de la responsabilité du trésorier et vice-trésorier.

Le support du site

Le groupe support du site, constitué d'une ou deux personnes au maximum, sont en charge du maintient des bases et de la sécurité des données. Ils ont donc, par la nature de leur fonction, accès à toutes les données. Ils doivent les protéger par tous les moyens qu'ils connaissent et appliquer à la lettre les règles imposées par le RGPD.

Si la situation l'imposait, notamment mais pas uniquement dans le cas où l'engagement de confidentialité détaillé ci-après n'était plus susceptible d'être respecté ou se trouvait menacé, ils ont la possibilité fonctionnelle de détruire l'ensemble des données personnelles rapidement et définitivement. Ils doivent alors exécuter cette action de manière préventive.

Accès légal

Il est rappelé que les données stockées sont soumises à la loi française et européenne.

Ceci implique que les forces de l'ordre et la justice, dûment habilitées, sont susceptibles d'exiger, légalement, d'avoir accès à ces données. Cette demande doit être faite selon les procédures exigées par la loi, et les informations fournies seront celles prévues par la loi, et uniquement celles-ci.

Le conseil de l'association serait bien évidemment impliqué dans toute procédure légale ayant cet objectif, afin de défendre les droits des inscrits et de l'association dans sa globalité.

Notre engagement de confidentialité

UNDIA s'engage à une politique de confidentialité très stricte. Les données confiées par nos inscrits sont donc protégées avec la plus grande attention, et suivent les engagements suivants.

Incessibilité

Les données personnelles que vous nous communiquez ne sont pas cessibles. Nous nous interdisons formellement de les communiquer à un tiers, quel qu'il soit. Elles ne peuvent donc être cédées, ou vendues à aucune entité, commerciale ou non.

Dans le cas d'une fusion avec une autre association, ce qui sera fait des données devra être soumis au vote des adhérents eux-mêmes, qui décideront comment procéder, selon le mode de scrutin prévu par les statuts de l'association.

Dans le cas d'une association nous rejoignant, il appartiendra aux adhérents et personnes concernées par l'intégration des données à nos serveurs de décider ce qui doit être fait des données. Si l'intégration est décidée, elle devra être soumise au préalable à l'acceptation sans réserve de cet engagement de confidentialité par tous les inscrits de l'association nous rejoignant, y compris les membres de cette association qui se retrouveraient en responsabilité dans la nouvelle entité.

La sécurité avant tout

Les données que vous nous confiez sont stockées dans une base sécurisée dont l'accès est restreint à deux personnes maximum (responsables du groupe web et support). Le site est conçu pour empêcher par défaut, dans son fonctionnement même, toute aspiration d'une partie ou de la totalité des données. Les informations accessibles sont compartimentées, ou soumises à des contraintes temporelles qui rendent extrêmement difficiles voire impossible des vols massifs de données.

Le système du site, est un système propriétaire qui n'est pas publiquement documenté, ce qui permet de limiter les failles découvertes par étude de code, qui sont souvent corrigées après les méfaits et qui restent parfois même inconnues sauf d'un tout petit groupe qui les exploite. Il a été codé avec les pratiques les plus sécurisées connues à ce jour.

Le site est hébergé sur un serveur qui utilise un certificat Let's Encrypt, afin de chiffrer par défaut toutes les communications entre l'utilisateur et le serveur,

pour le site et pour l'UNDIApp. Ceci pour éviter toute attaque du type « homme du milieu ».

La politique d'implémentation des mots de passe est très stricte. Les mots de passe des utilisateurs qui ont des fonctions officielles dans l'association sont personnels, différents les uns des autres et identifient donc formellement chaque utilisateur. Ils sont choisis aléatoirement parmi les 62 caractères usuels alphanumériques, augmentés des caractères spéciaux et accentués, pour être par défaut forts, et ainsi réduire le risque des attaques brutes de type clavier et/ou dictionnaire en augmentant considérablement le nombre de combinaisons possibles.

Les mots de passe maîtres et clés bancaires ont des longueurs supérieures à 15 caractères aléatoires, avec caractères spéciaux lorsque le système de notre hébergeur le permet, et sont tous différents. Ils sont changés régulièrement, et ne sont connus d'une seule personne.

Statistiques anonymisées

Pour mener à bien notre mission auprès des organismes et pouvoirs publics qui nous réglementent, nous pouvons avoir besoin de créer des statistiques sur nos adhérents et UNDIAmis. Ces statistiques sont traitées par le serveur automatiquement. Le code qui produit ces statistiques est conçu pour les purger de toute information personnelle avant même que le demandeur de ces statistiques (élus du bureau ou du CA) puisse les consulter.

En dernier recours, toute publication destiné à des entités extérieures à l'association, physique ou morale, doit être examinée par le groupe web et support qui se porte garant de l'absence de toute donnée qui pourrait identifier l'un de nos inscrits.

L'accès direct aux bases pour faire des études statistiques par une entité extérieure à l'association, morale ou physique, est formellement interdite.

Vos droits d'Adhérent et d'UNDIAmi

Le RGPD prévoit des droits que vous pouvez exercer auprès du groupe support et web de l'association (support@undia.fr). Ces droits peuvent être consultés dans le texte original du Règlement pour la Protection des Données Personnelles, n°2016/679 disponible sur les sources légales habituelles, entre autre le site de la CNIL.

Le droit à l'effacement

Vous pouvez demander l'effacement de toutes les données vous concernant stockées dans la base de données de l'association UNDIA. Le groupe support et web procédera à cet effacement sous 30 jours maximum. Cet effacement implique logiquement que votre accès à l'UNDIApp et/ou votre adhésion seront également supprimés, puisqu'il s'agit par nature de données personnelles stockées dans la base qui ne peuvent être maintenues seules.

6 motifs vous permettent d'invoquer cet effacement qui sont listés dans l'article 17 du RGPD, paragraphe 1 alinéas a-f, ils sont les suivants :

- les données collectées ne sont plus nécessaires ;
- vous retirez votre consentement donné lors de votre inscription ;
- vous vous opposez au traitement de ces données pour des raisons qui vous sont propres et qui peuvent être temporaires ;
- vous contestez l'exactitude des données ;
- les données concernent un mineur de moins de 16 ans dont les parents n'ont pas consenti au traitement des données, ou un mineur de moins de 13 ans ;
- les dispositions légales françaises demandent l'effacement de ces données.

La DI-008 de la CNIL, qui dispense de déclarer notre base à l'organisme de contrôle, nous impose justement une disposition légale supplémentaire par rapport au droit à l'effacement. Cette disposition dit que les données personnelles des anciens adhérents doivent être effacées après leur fin d'adhésion, que cette fin ait été volontaire (démission, non renouvellement de cotisation) ou imposée (radiation).

Pour des raisons pratiques (retard dans le renouvellement de cotisation), nous ne procédons à cet effacement que 30 jours après le non renouvellement de cotisation. En revanche, l'effacement est immédiat en cas de démission et de radiation.

Une partie des données peut être effacée par les inscrits eux-mêmes, sans nécessiter l'intervention du groupe web et support. Lorsque des données sont effacées, elles le sont immédiatement des bases utilisées par le site en production. Elles restent cependant stockées dans les bases de sauvegardes dites « snapshots », réalisées par notre hébergeur, pendant une durée de 31 jours, après quoi elles sont définitivement effacées lorsque la dernière sauvegarde les contenant est à son tour détruite.

Le droit à la portabilité

Vous pouvez demander la transmission des données à caractère personnel que vous avez stockées dans la base du site UNDIA. Ces données vous seront transmises dans un format lisible par une machine comme le prévoit la règle, afin d'être éventuellement importées dans d'autres services. Vu nos ressources limitées, nous ne pouvons pas nous charger du transfert de ces données dans le service que vous auriez choisi.

Par ailleurs nous ne pouvons techniquement pas créer des formats spécifiques à chaque service que vous souhaiteriez utiliser, cette transmission sera donc dans un format générique standard et structuré.

La portabilité ne concerne pas les données que vous avez entrées dans l'UNDIApp, puisque ces données ne sont pas stockées sur nos serveurs. Elles restent localement sur votre appareil, et sont donc de votre seule et unique responsabilité.

Le droit à la notification en cas de fuite

Nous protégeons au mieux de nos possibilités les données à caractère personnel que vous nous confiez. Cependant, le risque zéro n'existant pas, il est possible qu'une fuite de données se produise.

Nous mettons en place des systèmes de logs pour surveiller les accès et nous nous engageons à notifier les autorités compétentes immédiatement en cas de violations graves, et à vous notifier la nature de la fuite et ce qui a été dérobé dans la limite de ce que nous pouvons techniquement en connaître, le plus tôt possible.

Cette disposition vous permet de prendre les mesures adéquates pour vous protéger du vol en question.

La sécurité par défaut

L'ensemble de la conception du code du site UNDIA obéit à cette notion. Les fonctions et matrices fonctions/permissions reposent toutes sur l'idée qu'un accès peut être volé ou détourné, et donc à en limiter les conséquence au maximum, tout en laissant le site être fonctionnel.

Ceci implique que nous chiffrons les mot de passe avec des méthodes de haute sécurité et que nous exigeons de votre part l'utilisation de mots de passe complexes afin de réduire la surface d'attaque d'éventuelles personnes ou organismes mal intentionnés.

Ceci implique que les accès avec un haut niveau de fonctionnalité sont aussi plus sécurisés avec l'utilisation de l'authentification à deux facteurs.

Ceci implique que ces mêmes accès à haut niveau de fonctionnalité voient leur actions journalisées, afin qu'elles puissent être passées en revue, dans le but de détecter toute tentative d'intrusion.

Ceci implique que les mots de passe et clefs maîtres du site sont changés régulièrement.

Révisions

Ce document a été établi le 25 mai 2018 par UNDIA afin de réguler toutes les pratiques de l'association en ce qui concerne les données à caractère personnel, leur collecte, traitement et utilisation.

Il devra être révisé lorsque les dispositions légales l'exigeront. Il pourra être révisé sur demande du bureau ou du CA si ces organes estiment des changements nécessaires.

Dans tous les cas, lorsque les changements auront été actés, ils devront être soumis à l'acceptation de tous les inscrits sur le site UNDIA (UNDIAmis et adhérents), qui pourront alors décider, selon les dispositions légales, ce qui doit être fait de leurs données à caractère personnel.

Notre délégué à la protection des données

Le webmaster de notre site, Vincent Deville-Duc, qui a créé, codé et surveille le site UNDIA est notre délégué à la protection des données. Les demande au sujet des données à caractère personnel peuvent être adressées à support@undia.fr.