

Déploiement d'Office 365 en contexte scolaire Établissements publics ou structures privées exerçant des missions de service public

Document d'appui pour élaborer une demande d'avis sur un acte réglementaire à la CNIL

réalisé par DNE-A Numerilab du MENESR

personne à contacter : francois.bocquet@education.gouv.fr

Brouillon disponible jusqu'au 20 septembre en utilisant le code : **stG1755523B** à l'adresse
<https://www.cnil.fr/fr/declarer-un-fichier>

Menu du formulaire

<input checked="" type="checkbox"/> Changer de procédure
<input checked="" type="checkbox"/> Déclarant
<input checked="" type="checkbox"/> Mise en oeuvre
<input checked="" type="checkbox"/> Finalité
<input checked="" type="checkbox"/> Données traitées
<input checked="" type="checkbox"/> Données sensibles
<input checked="" type="checkbox"/> Sécurité
<input checked="" type="checkbox"/> Architecture
<input checked="" type="checkbox"/> Sécurité générale
<input checked="" type="checkbox"/> Sécurité préventive
<input checked="" type="checkbox"/> Authentification
<input checked="" type="checkbox"/> Sécurité cryptographique
<input checked="" type="checkbox"/> Transferts de données hors UE
<input checked="" type="checkbox"/> Transfert n° 1
<input checked="" type="checkbox"/> Interconnexions
<input checked="" type="checkbox"/> Droit d'accès
<input checked="" type="checkbox"/> Contact
<input checked="" type="checkbox"/> Identification du responsable
<input checked="" type="checkbox"/> Projet Acte Réglementaire (PAR)
<input checked="" type="checkbox"/> Validation et envoi

La structure du présent document reprend le menu du formulaire (sur la gauche de la page).

Déclarant :

renseigner le formulaire de façon complète

le déclarant est le responsable des traitements de données à caractère personnel

dans notre contexte c'est donc pour le moment :

- le chef d'établissement pour les collèges et les lycées ;
- le DASEN pour les écoles primaires (ou les IEN si ceux ci sont habilités par le DASEN à procéder aux démarches CNIL).

Mise en oeuvre :

cocher la première case puisque le chargé de la mise en oeuvre est identique au déclarant

Finalité :

Indiquer la finalité du traitement

- Mise à disposition des usagers d'un ou plusieurs téléservices de l'administration électronique
- Sûreté de l'Etat, défense, sécurité publique
- Prévention, recherche, constatation ou poursuite des infractions pénales ou exécution des condamnations pénales ou des mesures de sûreté
- Authentification ou contrôle de l'identité des personnes par un dispositif biométrique
- Vérification des identités par consultation du RNIPP
- Recensement de la population en métropole et dans les collectivités d'outre-mer
- Autre, précisez

Précisez la finalité du téléservice :

mettre à disposition des agents et des usagers (élèves) des services de messagerie, d'agenda incluant les tâches et de contacts, des portails collaboratifs (sites web et partage de vidéo), des outils de création de documents bureautiques en ligne (traitement de texte, tableur et visualisation, présentation, ...) et leur stockage partagé ou non (oneDrive), un réseau social fermé et supervisé et des outils d'audio et de visio-conférence, et enfin un moteur de recherche dans le périmètre contrôlé par l'instance Office 365. L'ensemble est articulé autour d'un annuaire dans le nuage (Azure AD) permettant de transmettre des jetons contenant ou non des vecteurs d'identité aux éventuels services tiers. L'ajout d'applications tierces est rendu possible de façon optionnelle par un magasin privé ou public d'applications.

Quel est l'objectif précis de votre traitement ?

Ex. : mise en oeuvre de plate-forme internet destinée à permettre aux usagers d'accomplir des démarches administratives ...

mise en oeuvre d'une plateforme collaborative pour produire et partager du contenu dans un contexte pédagogique au sein ou à l'extérieur de l'établissement scolaire (ou de l'école). Cette plateforme est particulièrement adaptée aux équipements individuels mobiles quels que soient les éditeurs de leurs écosystèmes. Chaque utilisateur ne peut accéder qu'aux seules informations auxquelles il a besoin d'accéder dans l'exercice de ses fonctions au sein de l'établissement.

Indiquer la finalité du traitement

Cocher : Mise à disposition des usagers d'un ou plusieurs téléservices de l'administration électronique

Précisez la finalité du téléservice :

“mettre à disposition des agents et des usagers (élèves) des services de messagerie, d'agenda incluant les tâches et de contacts, des portails collaboratifs (sites web et partage de vidéo), des outils de création de documents bureautiques en ligne (traitement de texte, tableur et visualisation, présentation, ...) et leur stockage partagé ou non (oneDrive), un réseau social fermé et supervisé et des outils d'audio et de visio-conférence, et enfin un moteur de recherche dans le périmètre contrôlé par l'instance Office 365. L'ensemble est articulé autour d'un annuaire dans le nuage (Azure AD) permettant de transmettre des jetons contenant ou non des vecteurs d'identité aux éventuels services tiers. L'ajout d'applications tierces est rendu possible de façon optionnelle par un magasin privé ou public d'applications.”

Quel est l'objectif précis de votre traitement ?

“mise en œuvre d'une plateforme collaborative pour produire et partager du contenu dans un contexte pédagogique au sein ou à l'extérieur de l'établissement scolaire (ou de l'école). Cette plateforme est particulièrement adaptée aux équipements individuels mobiles quels que soient les éditeurs de leurs écosystèmes. Chaque utilisateur ne peut accéder qu'aux seules informations auxquelles il a besoin d'accéder dans l'exercice de ses fonctions au sein de l'établissement.”

Les personnes peuvent-elles s'opposer à figurer dans ce traitement ? ?

Oui
 Non

Nom du logiciel ou de l'application concernée

Plateforme Office 365 pour l'Education de Microsoft

Quelles personnes sont concernées par le traitement ?

Salariés
 Usagers
 Adhérents
 Clients
 Visiteurs

Patients
 Etudiants/élèves
 Autres (précisez)

Si votre traitement recourt à technologie particulière, merci de préciser laquelle (facultatif) :

Dispositif sans contact (Ex : RFID,NFC)
 Carte à puce
 Vidéosurveillance
 Mécanisme d'anonymisation

Géo localisation
 Nanotechnologie
 Autres (précisez)

Les personnes peuvent-elles s'opposer à figurer dans ce traitement ?
cocher “oui”

Nom du logiciel ou de l'application concernée : “Plateforme Office 365 pour l'éducation de Microsoft”

Quelles personnes sont concernées par le traitement ?
cocher “salariés” et “étudiants/élèves”

Si votre traitement recourt à technologie particulière, merci de préciser laquelle (facultatif) :
cocher “géolocalisation”

Données traitées :

Etat-civil, identité, données d'identification

Etat-civil, identité, données d'identification

Détail, précisez :

- Nom, prénom
- Adresse
- Photographie
- Date, lieu de naissance
- Autres (précisez)

Origine ?

- Directement auprès de la personne concernée
- De manière indirecte, précisez

par importation/synchronisation de

Durée de conservation ?

jours mois années

Autres (précisez)

données conservées tant que l'utili

Destinataires ? (250 caract. max)

aucun

cocher "nom et prénom"

origine de manière indirecte : par importation/synchronisation de données depuis un annuaire ou un fichier csv

durée de conservation : données conservées tant que l'utilisateur est habilité puis données supprimées à T+90 jours

destinataires : aucun

Vie personnelle : ne rien cocher

Vie professionnelle

Vie professionnelle

Détail, précisez :

- CV
- Situation professionnelle
- Scolarité, formation
- Distinction
- Autres (précisez)

de façon optionnelle pour ce

Informations identiques à la rubrique précédente Oui

Cochez la case ci-dessus si les réponses sur l'origine, la durée de conservation et les destinataires sont les mêmes.

Origine ?

- Directement auprès de la personne concernée
- De manière indirecte, précisez

Durée de conservation ?

jours mois années

Autres (précisez)

idem (suppression en fin d'utilisati

Destinataires ? (250 caract. max)

néant

détail, cocher autres et précisez

"de façon optionnelle pour certaines briques applicatives (yammer, delve et mon compte)"

origine : Directement auprès de la personne concernée

durée de conservation : autre "idem (suppression en fin d'utilisation à T+90 jours, délai permettant la réactivation si erreur)"
destinataires : néant

Informations d'ordre économique et financier : ne rien cocher

Données de connexion (adresses Ip, logs, etc.)

Données de connexion (adresses Ip, logs, etc.)

Détail, précisez :

- Identifiants des terminaux
- Identifiants de connexions
- Informations d'horodatage
- Autres (précisez)

Autres (précisez)

Informations identiques à la rubrique précédente Oui

Cochez la case ci-dessus si les réponses sur l'origine, la durée de conservation et les destinataires sont les mêmes.

Origine ?

- Directement auprès de la personne concernée
- De manière indirecte, précisez

journalisation des connexions et de

Durée de conservation ? jours mois années

Autres (précisez)

idem que ci dessus. Journalisation

Destinataires (250 caract. max) ? néant (sauf requête judiciaire)

Détail, précisez :

cocher : Identifiants des terminaux, Identifiants de connexions, Informations d'horodatage
Origine : de manière indirecte "journalisation des connexions et détection du navigateur utilisé (ergonomie)"

Durée de conservation : autre "idem que ci dessus. Journalisation de sécurité sur 365 jours."

Destinataires : "néant (sauf requête judiciaire)"

Données de localisation (déplacements, données GPS, GSM, etc.)

Données de localisation (déplacements, données GPS, GSM, etc.)

Détail, précisez :

- Par satellite
- Par téléphone
- Autres (précisez)

Informations identiques à la rubrique précédente Oui
 Cochez la case ci-dessus si les réponses sur l'origine, la durée de conservation et les destinataires sont les mêmes.

Origine ?

- Directement auprès de la personne concernée
- De manière indirecte, précisez

Durée de conservation ? jours mois années

Autres (précisez)

Destinataires (250 caract. max) ?

Détail : autre "par l'adresse IP utilisée"

Origine : de manière indirecte "journalisation des connexions pour adaptation des services et détection de comportements frauduleux"

Durée de conservation : autres "idem (journalisation sur 365 jours et suppression à T+90 jours après désinscription du service)"

Destinataires : néant (sauf requête judiciaire)"

Données sensibles :

ne rien cocher sur les onglets

Sécurité :

Architecture :

Nom(s) du(des) système(s)

Nom(s) du(des) système(s) d'exploitation impliqués dans le traitement :

Le système informatique

Préciser le nombre de micro-ordinateurs, terminaux, téléphones ou PDA.



Préciser le type de micro-ordinateurs, terminaux, téléphones ou PDA.

Le système informatique est constitué :

D'un ou plusieurs serveurs, précisez s'ils sont :

Au sein de l'organisme

Externalisés

Autres architectures informatiques, précisez :

Le logiciel d'application met en oeuvre :

Précisez leur nom :

Une base de données :

Un infocentre :

Un logiciel d'analyse de données permettant d'effectuer des statistiques

Autres, précisez :

Nature du(des) réseau(x) informatique(s) de l'organisme utilisé(s) pour le traitement

Aucun réseau(par ex. élément autonome ou micro-ordinateur isolé)

Un ou plusieurs réseaux externalisés chez un prestataire

Un ou plusieurs réseaux sur un même site

Communications avec l'extérieur

Plusieurs réseaux distants interconnectés, précisez le mécanisme d'interconnexion :

Utilisation de technologies sans fil

Autres (précisez) :

Nom des systèmes :

Windows Serveur et VM Linux

Le système informatique

Préciser le nombre de micro-ordinateurs, terminaux, téléphones ou PDA.

(préciser selon les projets mis en oeuvre)

Préciser le type de micro-ordinateurs, terminaux, téléphones ou PDA.
(préciser selon les projets : nature des EIM, PC ou autres périphériques utilisés)

Le système informatique est constitué :
cocher "D'un ou plusieurs serveurs, précisez s'ils sont :
puis "Externalisés"

Autres architectures informatiques, précisez :
"architecture Cloud Office 365 (incluant Azure Active Directory)"

Le logiciel d'application met en oeuvre :
cocher : Une base de données : "SQL serveur dans infrastructure Cloud 365"
cocher : Un logiciel d'analyse de données permettant d'effectuer des statistiques
cocher : Un infocentre : "NOC/SOC d'Office 365 (Microsoft)"
cocher Autres, précisez : "Content Delivery NetWork (via Akamai pour l'habillage graphique)"

Nature du(des) réseau(x) informatique(s) de l'organisme utilisé(s) pour le traitement
cocher : Plusieurs réseaux distants interconnectés, précisez le mécanisme d'interconnexion
: "réseaux privés et/ou connexion VPN"
cocher : Un ou plusieurs réseaux externalisés chez un prestataire
cocher : Communications avec l'extérieur
cocher : Utilisation de technologies sans fil

Sécurité générale :

Sécurité générale

A savoir

Il convient de décrire la sécurité des échanges de données, les mesures de sécurité physique (les mesures de sécurité prévues pour l'accès aux bâtiments et aux équipements, la sécurité des services généraux, ...), et les méthodes de sauvegarde.

Entités et échanges

Si le traitement implique des échanges avec des utilisateurs, un hébergeur ou des tiers externes (organismes, partenaires, clients, ...) y compris à l'étranger :

Précisez les entités concernées par ces échanges :

la liste des sous-traitants est disponible <http://go.microsoft.com/fwlink/p/?LinkId=213175>

Echanges sur Internet (Web y compris par portail, Transfert de fichier, Email, ...). Précisez les protocoles et les mécanismes cryptographiques mis en oeuvre :

Un chiffrement des données entre poste et serveur et entre les serveurs ainsi que sur les postes et les serveurs est mis en oeuvre et documenté ici <http://go.microsoft.com/fwlink/p/?LinkId=401240>

Echanges sur un réseau privé. Type d'interconnexion (ex: VPN, LS):

tous les échanges sont réalisés via des réseaux privés de type LS.

Transfert de supports numériques ou analogiques (disque, bande, cd-rom, clé USB,...). Précisez le type de support et mécanismes cryptographiques :

néant

Autres (précisez) :

Précisez les entités concernées par ces échanges : "la liste des sous-traitants est disponible <http://go.microsoft.com/fwlink/p/?LinkId=213175>"

Echanges sur Internet (Web y compris par portail, Transfert de fichier, Email, ...). Précisez les protocoles et les mécanismes cryptographiques mis en oeuvre : "Un chiffrement des données entre poste et serveur et entre les serveurs ainsi que sur les postes et les serveurs est mis en oeuvre et documenté ici <http://go.microsoft.com/fwlink/p/?LinkId=401240>"

Echanges sur un réseau privé. Type d'interconnexion (ex: VPN, LS) : "tous les échanges sont réalisés via des réseaux privés de type LS."

Transfert de supports numériques ou analogiques (disque, bande, cd-rom, clé USB,...). Précisez le type de support et mécanismes cryptographiques : "néant"

Sécurité physique des locaux et des équipements

Décrivez la sécurité des locaux et équipements hébergeant le traitement (ex. clés, badge d'accès, gardiennage) :

la solution Office 365 est certifiée ISO 27001 et ISO 27018 (informations complémentaires sur <http://go.microsoft.com/fwlink/p/?LinkId=401240>)

Sauvegarde

Des mesures assurent la sauvegarde du système informatique. Veuillez décrire :

Le type de support :

disques durs dans les data-centers (plusi

La fréquence des sauvegardes :

sauvegarde en continue

La sécurité physique du lieu de stockage des supports :

cf <http://go.microsoft.com/fwlink/p/?LinkId>

Les mécanismes cryptographiques utilisés :

AES 256 bits

La sauvegarde est externalisée du système informatique :

Nom de l'hébergeur :

géré dans la solution Office 365 (hors agr

Sécurité physique des locaux et des équipements

Décrivez la sécurité des locaux et équipements hébergeant le traitement (ex. clés, badge d'accès, gardiennage) : "la solution Office 365 est certifiée ISO 27001 et ISO 27018 (informations complémentaires sur <http://go.microsoft.com/fwlink/p/?LinkId=401240>)"

Sauvegarde

Des mesures assurent la sauvegarde du système informatique. Veuillez décrire :

Le type de support : "disques durs dans les data-centers (plusieurs technos)"

La fréquence des sauvegardes : "sauvegarde en continue"

La sécurité physique du lieu de stockage des supports : "cf <http://go.microsoft.com/fwlink/p/?LinkId=401240>"

Les mécanismes cryptographiques utilisés : "AES 256 bits"

Cocher : La sauvegarde est externalisée du système informatique :

Nom de l'hébergeur : "géré dans la solution Office 365 (hors agrément SIAF)"

Sécurité préventive

Protection contre les intrusions

Plusieurs moyens possibles

- Un antivirus est installé sur tous les postes prenant part au traitement
- Un système de détection d'intrusion (IDS) est utilisé. Nom :
- Une compartimentation du réseau avec des règles de filtrage est effectuée (ex. DMZ, firewall)
- Le traitement est confiné dans un ou plusieurs réseaux isolés des autres traitements (ex. VLAN)
- Autres (précisez) :

Protection contre les intrusions

Plusieurs moyens possibles

cocher : Un système de détection d'intrusion (IDS) est utilisé. Nom : "liste de contrôle d'accès à plusieurs niveaux"

cocher : Une compartimentation du réseau avec des règles de filtrage est effectuée (ex. DMZ, firewall)

cocher : Le traitement est confiné dans un ou plusieurs réseaux isolés des autres traitements

Mesures

Mesures pour assurer la confidentialité des données lors du développement de l'application informatique :

- Les environnements de développement et de production sont distincts
- Les personnels affectés aux tâches de développement et de gestion/exploitation sont distincts
- La mise au point des logiciels s'effectue sur des données :
 - Anonymisées
 - Fictives
- Autres (précisez)

Mesures pour assurer la confidentialité des données lors du opération de maintenances des logiciels ou des équipements :

- Les interventions de maintenance sont enregistrées dans une main-courante
- Les logiciels ou équipements informatiques font l'objet d'une télémaintenance

Mesures de sécurité appliquées lors de ces opérations :

permissions particulières pour chaque type de tâches et actions nominatives et journalisées.

Procédure particulière si la télémaintenance nécessite un accès aux fichiers de données à caractère personnel :

oui, accès restreint à des ingénieurs disposant de certifications internes pour agir sur des données personnelles et audit avec certification ISO 27018

- La maintenance des matériels par un sous-traitant est faite en présence d'un informaticien de l'entreprise
- Les supports de stockage envoyés à l'extérieur pour réparation font l'objet d'une procédure de protection :

pas de réparation : en cas de défaillance l'intégralité du composant (disque, rack, ...) est remplacé.

- Les supports de stockage destinés à la destruction font l'objet d'une procédure de protection particulière :

disques durs chiffrés par Bitlocker AES 256 bits puis fichiers morcellés (récupération impossible par un tiers).

Mesures

Mesures pour assurer la confidentialité des données lors du développement de l'application informatique :

Cocher : Les environnements de développement et de production sont distincts

Cocher : Les personnels affectés aux tâches de développement et de gestion/exploitation sont distincts

Cocher : La mise au point des logiciels s'effectue sur des données :

cocher : Fictives

Mesures pour assurer la confidentialité des données lors du opération de maintenances des logiciels ou des équipements :

cocher : Les interventions de maintenance sont enregistrées dans une main-courante

cocher : Les logiciels ou équipements informatiques font l'objet d'une télémaintenance

Mesures de sécurité appliquées lors de ces opérations : "permissions particulières pour chaque type de tâches et actions nominatives et journalisées."

Procédure particulière si la télémaintenance nécessite un accès aux fichiers de données à caractère personnel : "oui, accès restreint à des ingénieurs disposant de certifications internes pour agir sur des données personnelles et audit avec certification ISO 27018"

cocher : La maintenance des matériels par un sous-traitant est faite en présence d'un informaticien de l'entreprise

cocher : Les supports de stockage envoyés à l'extérieur pour réparation font l'objet d'une procédure de protection : "pas de réparation : en cas de défaillance l'intégralité du composant (disque, rack, ...) est remplacé."

cocher : Les supports de stockage destinés à la destruction font l'objet d'une procédure de protection particulière : "disques durs chiffrés par Bitlocker AES 256 bits puis fichiers morcelés (récupération impossible par un tiers)."

Authentification

Authentification

Authentification/identification des personnes habilitées à accéder à l'application (plusieurs choix possibles) :

Des profils d'habilitation définissent les fonctions ou les types d'informations accessibles à un utilisateur

Le contrôle d'accès logique se fait :

par un mot de passe. Quelles sont ses caractéristiques (structure obligatoire, durée de validité, etc.) : ?

la longueur et la composition des mots de passe ainsi que la durée de vie de ce dernier, son historique, la durée de son historique ainsi que le nombre de tentative sont défini par l'administrateur

par un dispositif matériel non-biométrique (ex. carte à puce). Précisez son nom et s'il est complété par la saisie d'un code secret ou PIN : ?

possible d'activer une identification multi-facteur via SMS, carte à puce, clé USB, clé OTP (tout périphérique compatible STS) -> non prévu dans la version éducation gratuite.

par un dispositif biométrique. Précisez lequel : ?

au moyen de certificats logiciels « client » ?

par un autre mécanisme. Précisez lequel : ?

Décrivez brièvement la procédure de distribution des moyens de contrôle d'accès aux personnes habilitées : ?

plusieurs de type de profils sont utilisés :
Utilisateur (sans droits)
Administrateur général, admin personnalisé selon services et selon population supervisée
-> archivage legal Ediscovery (avec RSSI)

Authentification/identification des personnes habilitées à accéder à l'application (plusieurs choix possibles) :

Cocher : Des profils d'habilitation définissent les fonctions ou les types d'informations accessibles à un utilisateur

Le contrôle d'accès logique se fait :

Cocher : par un mot de passe. Quelles sont ses caractéristiques (structure obligatoire, durée de validité, etc.) : "la longueur et la composition des mots de passe ainsi que la durée de vie de ce dernier, son historique, la durée de son historique ainsi que le nombre de tentative sont défini par l'administrateur"

Cocher : par un dispositif matériel non-biométrique (ex. carte à puce). Précisez son nom et s'il est complété par la saisie d'un code secret ou PIN : "possible d'activer une identification multi-facteur via SMS, carte à puce, clé USB, clé OTP (tout périphérique compatible STS) -> non prévu dans la version éducation gratuite."

Cocher : Décrivez brièvement la procédure de distribution des moyens de contrôle d'accès aux personnes habilitées : "plusieurs de type de profils sont utilisés :

Utilisateur (sans droits)

Administrateur général, admin personnalisé selon services et selon population supervisée

-> archivage legal Ediscovery avec RSSI"

Journalisation

Certaines données font l'objet d'une journalisation :

<p>Accès à l'application</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Date/heure de connexion<input checked="" type="checkbox"/> Identifiant du poste de travail<input checked="" type="checkbox"/> Identifiant de l'utilisateur<input checked="" type="checkbox"/> Date/heure de déconnexion<input checked="" type="checkbox"/> Opération effectuée<input type="checkbox"/> Autres (précisez) : <input type="text"/>	<p>Accès aux fichiers de données à caractère personnel</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Date/heure de connexion<input checked="" type="checkbox"/> Identifiant du poste de travail<input checked="" type="checkbox"/> Identifiant de l'utilisateur<input checked="" type="checkbox"/> La référence des données accédées<input type="checkbox"/> Autres (précisez) : <input type="text"/> <p>Type d'accès journalisés, pour :</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Consultation<input checked="" type="checkbox"/> Création<input checked="" type="checkbox"/> Mise à jour<input checked="" type="checkbox"/> Suppression<input type="checkbox"/> Autres (précisez) : <input type="text"/>
---	---

Journalisation

Certaines données font l'objet d'une journalisation :

Accès à l'application :

cocher : Date/heure de connexion

cocher : Identifiant du poste de travail

cocher : Identifiant de l'utilisateur

cocher : Date/heure de déconnexion

cocher : Opération effectuée

Accès aux fichiers de données à caractère personnel

cocher : Date/heure de connexion

cocher : Identifiant du poste de travail

cocher : Identifiant de l'utilisateur

cocher : La référence des données accédées

Type d'accès journalisés, pour :

cocher : Consultation

cocher : Création

cocher : Mise à jour

cocher : Suppression

Sécurité cryptographique :

Sécurité cryptographique

A savoir

Il convient de décrire les algorithmes cryptographiques mis en oeuvre.

Confidentialité/intégrité

L'application met en oeuvre des procédés :

D'anonymisation des données. ?

Nom du procédé :

De chiffrement des données à caractère personnel stockées ?

Algorithme (Ex. 3DES) :

Longueur de la clé :

De contrôle d'intégrité des données à caractère personnel stockées ?

Algorithme (Ex. HMAC) :

Longueur de la clé :

De sécurisation du transport des données à caractère personnel ?

Protocole de sécurisation (Ex. SSLv3):

D'authentification destinataire ou "serveur" (signature électronique, certificat,...) ?

Procédé et nom commercial :

D'authentification émetteur ou "client" (signature électronique, certificat,...) ?

Procédé et nom commercial :

Confidentialité/intégrité

Cocher : De chiffrement des données à caractère personnel stockées

Algorithme (Ex. 3DES) : AES

Longueur de la clé : 256 bits

Cocher : De contrôle d'intégrité des données à caractère personnel stockées

Algorithme (Ex. HMAC) : AES (respecte la norme FIPS 140-2)

Longueur de la clé : 256 bits

Cocher : De sécurisation du transport des données à caractère personnel

Protocole de sécurisation (Ex. SSLv3) : TLS v1.2 clé à 2048 bits et PFS (perfect forward secrecy)

Transfert hors UE :

Destination des données

Sélectionnez un pays à ajouter

- Australie
- Etats-Unis d'Amérique
- Inde
- Singapour
- Hong-Kong

Type de destinataire

Veillez préciser la nature du lien juridique qui le relie au responsable de traitement

Maison mère

Filiale

Prestataire

Partenaire commercial

Autre

Quelle est la finalité du transfert ?

Ex. : centrale d'appel, assistance clientèle, saisie des données, ...

localisation de la passerelle Azure AD sur l'ensemble des data-centers et de services Yammer et Sway aux US ainsi que transfert d'information au support d'administration à la demande de l'administrateur (localisation selon l'horaire). Les autres traitements sont réalisés en Europe.

ATTENTION, si vous transférez des données pour des finalités distinctes, vous devez créer une annexe pour chaque finalité de transfert hors UE.
(ex : finalités d'hébergement de données et de saisie de données = 2 annexes).

Pays à ajouter :

- Australie
- Etats-Unis d'Amérique
- Inde
- Singapour
- Hong-Kong

Type de destinataire : Prestataire

Quelle est la finalité du transfert ?

“ocalisation de la passerelle Azure AD sur l'ensemble des data-centers et de services Yammer et Sway aux US ainsi que transfert d'information au support d'administration à la demande de l'administrateur (localisation selon l'horaire). Les autres traitements sont réalisés en Europe.”

Quelles sont les catégories des personnes concernées par le transfert ?

- | | |
|--|--|
| <input checked="" type="checkbox"/> Salariés | <input checked="" type="checkbox"/> Etudiants/élèves |
| <input type="checkbox"/> Usagers | <input type="checkbox"/> Clients |
| <input type="checkbox"/> Adhérents | <input type="checkbox"/> Visiteurs |
| <input type="checkbox"/> Patients | <input type="checkbox"/> Autres (précisez) |

Quelle est la nature des traitements opérés par les destinataires des données ?

Ex. : lecture seule, saisie...

sous traitant assurant la fourniture des services ou le support.

Quelles sont les catégories des données transférées ?

- | | |
|--|--|
| <input checked="" type="checkbox"/> Etat-civil/identité/données d'identification | <input type="checkbox"/> N° de sécurité sociale |
| <input type="checkbox"/> Vie personnelle | <input type="checkbox"/> Données génétiques |
| <input type="checkbox"/> Vie professionnelle | <input type="checkbox"/> Appréciations sur les difficultés sociales des personnes |
| <input type="checkbox"/> Informations d'ordre économique et financier | <input type="checkbox"/> Origines raciales, ethnique, opinions politiques, philisophiques, religieuses, appartenance syndicale, vie sexuelle |
| <input checked="" type="checkbox"/> Données de connexion | <input type="checkbox"/> Données biométriques |
| <input checked="" type="checkbox"/> Données de localisation | <input type="checkbox"/> Infractions, condamnations, mesures de sûreté |
| | <input type="checkbox"/> Données de santé |

Quelles sont les catégories des personnes concernées par le transfert ?

- Salariés
- Etudiants/élèves

Quelle est la nature des traitements opérés par les destinataires des données ?

- sous traitant assurant la fourniture des services ou le support.

Quelles sont les catégories des données transférées ?

- Etat-civil/identité/données d'identification
- Données de connexion
- Données de localisation

NB : le contrat complet comportant en annexe les clauses de contrat type

Quelles sont les garanties mises en oeuvre pour permettre le transfert

- Niveau de protection suffisant
- Contrat de responsable de traitement à responsable de traitement (clauses contractuelles types de la Commission européenne) ?
- Contrat de responsable de traitement à sous-traitant (clauses contractuelles types de la Commission européenne)
- Certification "Safe Harbor" (concerne uniquement les Etats-Unis) ?
- BCR - Responsable de traitement du groupe
Nom du groupe d'entreprises :
- BCR - Sous-traitant du groupe
Nom du groupe d'entreprises :
- Un des cas prévus par l'article 69 de la loi du 6 janvier 1978 modifiée, précisez lequel : ?
 - Conclusion ou l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et un tiers
 - Consentement de la personne
 - Consultation d'un registre public
 - Exécution d'un contrat entre le responsable du traitement et l'intéressé
 - Respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice
 - Sauvegarde de l'intérêt public
 - Sauvegarde de la vie de la personne

Quelles sont les garanties mises en oeuvre pour permettre le transfert

- Contrat de responsable de traitement à sous-traitant (clauses contractuelles types de la Commission européenne)

Interconnexions :

Interconnexions

A savoir

Cette rubrique est à remplir si vous procédez à des échanges de données entre fichiers.

Procédez-vous à des interconnexions de fichiers ayant des finalités différentes ou poursuivant un intérêt public différent ?

- Oui
 Non

Procédez-vous à des interconnexions de fichiers ayant des finalités différentes ou poursuivant un intérêt public différent ?

- Non

Droit d'accès :

Champs obligatoires

Comment informez-vous les personnes concernées par votre traitement de leur droit d'accès ?

Mentions légales sur le formulaire Affichage

Mentions sur le site internet Envoi d'un courrier personnalisé

Autres (précisez)

charte signée par les élèves et leurs resp

Organisme chargé du droit d'accès

Cochez ci-contre si le chargé du droit d'accès est identique au déclarant

Cochez ci-contre si le chargé du droit d'accès est une personne physique (à titre individuel)

N° SIREN + NIC

Code NAF/APE

Nom de l'organisme

Nom du service

Adresse

Code Postal

Ville

Sigle

Téléphone

Télécopie

Adresse électronique

Comment informez-vous les personnes concernées par votre traitement de leur droit d'accès ?

- Mentions sur le site internet
- Autres (précisez) : "charte signée par les élèves et leurs responsables légaux et par les enseignants"

Organisme chargé du droit d'accès : cocher la première case "si le chargé du droit d'accès est identique au déclarant"

Contact :

placer dans cette page les informations relatives à la personne qui pourrait répondre au question de la CNIL

le plus logique est de placer les références du déclarant (chef d'établissement ou DASEN selon les cas) et de cocher la case qui demande à ce que cette personne soit destinataire du récépissé de la CNIL.

Engagement du responsable :

cocher la case “Je m'engage à ce que le traitement décrit par ce formulaire respecte les exigences de la loi du 6 janvier 1978 modifiée.”

les informations devraient être celle du chef d'établissement ou du DASEN

Projet d'acte réglementaire :

vous pouvez générer votre projet d'acte réglementaire que vous allez télécharger.

Vous pourrez alors l'éditer pour l'adapter à votre contexte

ensuite vous pouvez le téléverser par l'étape 3 depuis votre ordinateur vers le site de la CNIL (cliquer sur “choisissez un fichier”, sélectionner le fichier mis à jour (si possible en version pdf) puis cliquer sur “ajouter”. Le transfert de votre acte réglementaire remonte alors à la CNIL.

Validation et envoi :

un rappel avec d'éventuels manques dans les pages du formulaire vous est proposé.

Les compléter le cas échéant puis...

Suivre ensuite la procédure de validation définitive.