

POLITIQUE DE COLLECTE ET UTILISATION DE VOS DONNEES PERSONNELLES - eCandidat

I- Traitement des données à caractère personnel obligatoire

PRINCIPES GENERAUX

Le Règlement (EU) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, autrement appelé le Règlement Général sur la Protection des Données (ci-après RGPD) fixe le cadre juridique applicable aux traitements de données à caractère personnel.

Pour satisfaire à son bon fonctionnement, l'Université Paris-Saclay est tenue de mettre en œuvre et d'exploiter des traitements de données à caractère personnel relatifs aux étudiants et stagiaires formés, ainsi qu'aux candidats qui postulent.

RESPONSABLE DE TRAITEMENT ET COORDONNEES

Université Paris-Saclay

3 rue Joliot Curie

Bâtiment Breguet

91190 Gif-sur-Yvette

FINALITES ET BASE LEGALES

Vos données personnelles peuvent être collectées pour les finalités suivantes :

1. Assurer la gestion des candidatures (Mission d'intérêt public).
2. Assurer la gestion administrative de l'étudiant (Obligation légale et mission d'intérêt public).
3. Assurer l'inscription de l'étudiant (Obligation légale).
4. Permettre à l'outil de candidature, la création et la gestion d'un compte utilisateur (Intérêt légitime).

5. Permettre les remontées d'informations obligatoires à des fins d'études et de statistiques (enquête des organismes de l'État et études internes => intérêt légitime).
6. Permettre la mise en œuvre de l'accueil des étudiants sur le campus (Mission de service public).
7. Permettre à l'issue de votre scolarité de vous inviter à la cérémonie de remise de diplômes à partir de votre adresse électronique personnelle (Intérêt légitime).
8. Permettre au personnel de recrutement de proposer une bourse (Intérêt légitime).

DESTINATAIRES DES DONNEES PERSONNELLES

L'Université Paris-Saclay s'assure que les données ne soient accessibles qu'à des destinataires internes ou externes autorisés. L'Université Paris-Saclay peut faire appel à des prestataires externes n'agissant que sur instruction de l'Université Paris-Saclay et n'ayant accès aux données à caractère personnel des utilisateurs que pour exécuter les services demandés.

Destinataires internes :

-Les personnels administratifs des composantes et des services centraux et enseignants habilités par l'Université Paris-Saclay.

Destinataires externes :

-Les prestataires de services de l'Université Paris-Saclay (organismes de labellisation, certification, fournisseurs de systèmes d'informations, etc.).

-Les éditeurs de contenus ou de services pédagogiques liés à l'Université Paris-Saclay.

-Les autorités de tutelle : Ministère de l'Enseignement Supérieur et de la Recherche, Rectorat.

-Tout destinataire exerçant un mandat légal et pouvant exiger des informations personnelles (tribunaux, services de l'État, etc.).

-Universités et écoles partenaires de l'Université Paris-Saclay, notamment universités et partenaires étrangers hors UE.

TRANSFERT DE DONNEES

Aucun transfert de données n'est effectué en dehors de l'Union Européenne excepté dans le cadre d'années effectuées à l'étranger. Dans ce dernier cas,

l'Université Paris-Saclay veille à ce que le transfert soit encadré conformément au RGPD,

DUREE DE CONSERVATION

Pour les candidats classés sans suite, le dossier est conservé jusqu'à extinction des voies de recours et pour une durée maximale de deux ans après la clôture de la campagne de candidature.

Pour les candidats admis, les données de candidature sont conservées pour une durée maximale de deux ans après la clôture de la campagne de candidature.

Pour les candidats admis, elles sont ensuite conservées pour une durée de 50 ans conformément aux règles définies dans l'instruction Culture DAF/DPACI/RES/2005/003 du 22 Février 2005.

SECURITE

L'Université Paris-Saclay s'attache à préserver la confidentialité, l'intégrité et la disponibilité de vos données, et met en œuvre des mesures de sécurité techniques, logistiques et organisationnelles adaptées. Ces mesures assurent un niveau de sécurité adapté aux risques qui accompagnent le traitement de vos données à caractère personnel et, en tout état de cause, des données fournies.

DONNEES COLLECTEES

En cas de non fourniture des données obligatoires, la candidature ne pourra pas être traitée ou entraînera du retard dans le traitement du dossier.

Les données obligatoires collectées sont indiquées par une étoile rouge au-dessus de chaque libellé :

Civilité, Nom, prénom, date de naissance, ville, département et pays de naissance, nationalité, adresse complète, année d'obtention, série, mention du baccalauréat, ou équivalent, pays d'obtention du baccalauréat ou équivalent, établissement, adresse et éventuelles spécialités pour les baccalauréats français. Diverses pièces justificatives obligatoires requises selon les formations (exemples : CV, Lettre de Motivation, lettre de recommandation, diplômes obtenus, relevés de notes, relevés du baccalauréat, certificat de scolarité, ...),

Les données facultatives collectées sont :

Nom usuel, autre prénom, téléphone, téléphone portable, INE, options des baccalauréats français,

cursus actuel et cursus antérieurs, informations sur les stages effectués (année, organisme, durée, nombre d'heure, sujet du stage), expérience professionnelle (année, organisme, durée, , sujet , mission), divers justificatifs recommandés mais non obligatoires

VIOLATION DES DONNÉES

En cas de violation de données à caractère personnel, l'Université Paris-Saclay s'engage à en notifier à la CNIL dans les conditions prescrites par la réglementation en vigueur.

Lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, celles-ci sont également informées dans les conditions prévues par la réglementation.

EXERCICE DE VOS DROITS

Conformément à la loi du 6 janvier 1978 modifiée dite « Informatique et Libertés » et au Règlement (UE) 2016/679 du 27 avril 2016 dit « RGPD », vous disposez sur vos données, d'un droit d'accès, de rectification, de limitation, de portabilité, d'opposition et d'effacement.

Pour exercer ces droits, vous pouvez envoyer un message en justifiant votre identité et en écrivant à notre DPO via le mail suivant : dpd@universite-paris-saclay.fr, ou par courrier postal à l'adresse suivante : 3, rue Juliot Curie, 91190 Gif sur Yvette.

Si vous estimez, après nous avoir contactés, que vos droits ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL sur son site internet : <https://www.cnil.fr/fr/agir> ou par courrier : Commission Nationale de l'Informatique et des Libertés, 3 Place de Fontenoy - TSA 80715, 75334 PARIS CEDEX 07.

ÉVOLUTION

La présente politique peut être modifiée ou aménagée à tout moment en cas d'évolution légale, jurisprudentielle, des décisions et recommandations de la CNIL ou des usages.

Règles de sécurité et de confidentialité attendues dans le cadre de leurs fonctions

L'Université met en œuvre l'ensemble des mesures techniques et organisationnelles nécessaires pour assurer la sécurité, la confidentialité et l'intégrité des données traitées.

Conditions d'accès

L'accès aux outils, locaux, applications et données est strictement réservé aux agents autorisés dans le cadre de leurs missions.

Chaque agent dispose d'un compte nominatif, personnel et non transférable. Le partage d'identifiants ou de mots de passe est interdit.

Les droits d'accès sont définis selon le principe du "moindre privilège" : seuls les accès nécessaires à l'exercice des missions sont accordés.

En cas de départ, de mobilité ou d'absence prolongée, les accès doivent être désactivés ou ajustés sans délai.

Limitation d'usage

Les informations, documents et outils mis à disposition dans le cadre du travail ne peuvent être utilisés qu'à des fins professionnelles.

Toute utilisation à titre personnel, commercial ou extérieur à la mission est interdite.

Les agents et utilisateurs s'engagent à ne pas copier, transférer ni diffuser de données internes sur des supports ou espaces non sécurisés (clé USB personnelle, messagerie privée, cloud non autorisé, etc.).

Les traitements de données personnelles doivent respecter le RGPD et les règles internes de confidentialité (registre des traitements, mentions d'information, durée de conservation, etc.).

En cas de doute, d'incident de sécurité ou de perte de données, le supérieur hiérarchique et le DPO doivent être informés immédiatement.

