Oleo

Version du 12 novembre 2026
oleo-app.fr/securite

Contrat de sous-traitance

Clauses contractuelles types de la Commission européenne entre responsable du traitement et sous-traitant, pour l'usage d'Oléo par les enseignants de votre établissement.

Comment lire ce contrat

1. Les clauses ci-dessous sont celles de la **décision d'exécution (UE) 2021/915** de la Commission du 4 juin 2021 (JO L 199 du 7.6.2021, p. 18), reproduites **sans modification** d'après le Journal officiel de l'Union européenne. Seules ont été retenues les options que le texte propose lui-même : le règlement (UE) 2016/679 (RGPD) partout, et, à la clause 7.7, l'autorisation écrite générale des sous-traitants ultérieurs, avec une information trente jours à l'avance.
2. Les **annexes I à IV**, seules parties que les clauses permettent de compléter, ont été remplies par FLUOW, éditeur d'Oléo. Les cases en pointillé relèvent de l'établissement.
3. Le responsable du traitement est l'établissement ; FLUOW est le sous-traitant pour les données des élèves. Le contrat se signe à l'annexe I.

Clauses contractuelles types

SECTION I

Clause 1 Objet et champ d'application

a) Les présentes clauses contractuelles types (ci-après les «clauses») ont pour objet de garantir la conformité avec l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

b) Les responsables du traitement et les sous-traitants énumérés à l'annexe I ont accepté ces clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 et/ou des dispositions de l'article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725.

c) Les présentes clauses s'appliquent au traitement des données à caractère personnel tel que décrit à l'annexe II.

d) Les annexes I à IV font partie intégrante des clauses.

e) Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

f) Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

Clause 2 Invariabilité des clauses

a) Les parties s'engagent à ne pas modifier les clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent.

b) Les parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

Clause 3 Interprétation

a) Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 ou dans le règlement (UE) 2018/1725 figurent dans les clauses, ils s'entendent comme dans le règlement en question.

b) Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679 et du règlement (UE) 2018/1725 respectivement.

c) Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 / le règlement (UE) 2018/1725 ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

Clause 4 Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

Clause 5 — Facultative Clause d'amarrage

a) Toute entité qui n'est pas partie aux présentes clauses peut, avec l'accord de toutes les parties, y adhérer à tout moment, en qualité soit de responsable du traitement soit de sous-traitant, en complétant les annexes et en signant l'annexe I.

b) Une fois que les annexes mentionnées au point a) sont complétées et signées, l'entité adhérente est considérée comme une partie aux présentes clauses et jouit des droits et est soumise aux obligations d'un responsable du traitement ou d'un sous-traitant, conformément à sa désignation à l'annexe I.

c) Les présentes clauses ne créent pour la partie adhérente aucun droit ni aucune obligation pour la période précédant l'adhésion.

SECTION II – OBLIGATIONS DES PARTIES

Clause 6 Description du ou des traitements

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés à l'annexe II.

Clause 7 Obligations des parties

7.1. Instructions

a) Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

b) Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 / du règlement (UE) 2018/1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

7.2. Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l'annexe II, sauf instruction complémentaire du responsable du traitement.

7.3. Durée du traitement des données à caractère personnel

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée à l'annexe II.

7.4. Sécurité du traitement

a) Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.

b) Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

7.5. Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

7.6. Documentation et conformité

a) Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.

b) Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.

c) Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.

d) Le responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.

e) Les parties mettent à la disposition de l'autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

7.7. Recours à des sous-traitants ultérieurs

a) **AUTORISATION ÉCRITE GÉNÉRALE:** le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins trente jours à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition.

b) Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

c) À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.

d) Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

e) Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

7.8. Transferts internationaux

a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725.

b) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

Clause 8 Assistance au responsable du traitement

a) Le sous-traitant informe sans délai le responsable du traitement de toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l'y ait autorisé.

b) Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits, en tenant compte de la nature du traitement. Dans l'exécution de ses obligations conformément aux points a) et b), le sous-traitant se conforme aux instructions du responsable du traitement.

c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant:

   1) l'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel («analyse d'impact relative à la protection des données») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques;

   2) l'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque;

   3) l'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes;

   4) les obligations prévues à l'article 32 du règlement (UE) 2016/679.

d) Les parties définissent à l'annexe III les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

Clause 9 Notification de violations de données à caractère personnel

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679 ou des articles 34 et 35 du règlement (UE) 2018/1725, selon celui qui est applicable, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

9.1. Violation de données en rapport avec des données traitées par le responsable du traitement

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement:

a) aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le responsable du traitement en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques);

b) aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable du traitement, et inclure, au moins:

   1) la nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

   2) les conséquences probables de la violation de données à caractère personnel;

   3) les mesures prises ou les mesures que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais;

c) aux fins de la satisfaction, conformément à l'article 34 du règlement (UE) 2016/679, de l'obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

9.2. Violation de données en rapport avec des données traitées par le sous-traitant

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe le responsable du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins:

a) une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés);

b) les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel;

c) ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les parties définissent à l'annexe III tous les autres éléments que le sous-traitant doit communiquer lorsqu'il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679.

SECTION III – DISPOSITIONS FINALES

Clause 10 Non-respect des clauses et résiliation

a) Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.

b) Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si:

   1) le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au point a) et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;

   2) le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725;

   3) le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

c) Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.

d) À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

Texte officiel : décision d'exécution (UE) 2021/915, eur-lex.europa.eu/eli/dec_impl/2021/915/oj.

Annexe I — Liste des parties

Responsable du traitement

Nom	À compléter par l'établissement — l'établissement
Adresse	À compléter par l'établissement
Nom, fonction et coordonnées de la personne de contact	À compléter par l'établissement — le chef d'établissement, ou le DASEN pour une école
Délégué à la protection des données	À compléter par l'établissement — le DPD de l'académie
Signature et date d'adhésion	

Sous-traitant

Nom	FLUOW, société par actions simplifiée unipersonnelle au capital de 1 000 €, SIREN 943 565 531 RCS Manosque, éditrice d'Oléo
Adresse	49 chemin des Chambarels, 04300 Forcalquier
Nom, fonction et coordonnées de la personne de contact	Sarah Taisne, présidente · contact@fluow-design.fr · formulaire de contact d'oleo-app.fr
Signature et date d'adhésion	

Annexe II — Description du traitement

Catégories de personnes concernées	Les élèves des classes des enseignants de l'établissement qui utilisent Oléo.
Catégories de données traitées	Identité : nom, prénom, date de naissance. Scolarité : classe et groupes. Genre. Indication d'un accompagnement par un·e AESH. Besoin d'être placé aux deux premiers rangs, et place sur les plans de classe. Annotations posées par l'enseignant (catégorie qu'il a choisie, nombre, date) et remarques libres qui les accompagnent. Mémos de classe, qui peuvent nommer des élèves.
Données sensibles, limitations et garanties	Aucune donnée sensible n'est demandée. L'indication d'un accompagnement par un·e AESH, ou d'un besoin d'être placé aux premiers rangs, peut toutefois révéler une situation de handicap ou de santé, et une remarque libre peut en contenir selon ce que l'enseignant y écrit. Garanties appliquées : finalité strictement limitée au cours de l'enseignant ; accès réservé au seul enseignant titulaire du compte, sans aucun partage ; noms, prénoms, dates de naissance et mémos chiffrés ; durée de conservation fixée une fois pour toutes, avec effacement automatique ; aucun transfert hors de l'Union européenne.
Nature du traitement	Hébergement, enregistrement, organisation, consultation, modification, affichage, sauvegarde, conservation et effacement des données, à l'initiative de l'enseignant, dans une application en ligne. Les données sont saisies par l'enseignant ou importées par lui depuis le fichier exporté de Pronote.
Finalité	Permettre à l'enseignant de préparer et de conduire ses cours : plans de classe et placement des élèves, annotations en classe et leur suivi, mémos, emploi du temps.
Durée du traitement	Pendant toute la durée d'utilisation d'Oléo par les enseignants de l'établissement. Les données des élèves d'une classe sont conservées pendant son année scolaire et toute l'année suivante, puis effacées automatiquement le 1er août ; l'enseignant peut les supprimer plus tôt, à tout moment, et la suppression de son compte efface toutes ses données. Les sauvegardes sont conservées 30 jours sur le serveur, et supprimées de l'ordinateur de l'éditeur au-delà de 90 jours ou de 120 copies.
Sous-traitant ultérieur : objet, nature, durée	o2switch (annexe IV) : hébergement de l'application, de sa base de données et de ses sauvegardes sur le serveur, en France, et envoi des courriels de connexion, pour la durée du traitement.
Hors du champ des présentes clauses	Le compte de l'enseignant (adresse e-mail, mot de passe, nom, prénom, mesure de l'usage), dont FLUOW est responsable du traitement. À ce titre, lorsqu'un enseignant dépose son emploi du temps en image ou en PDF, ce fichier, qui ne contient aucune donnée d'élève et n'est pas conservé, est lu par Anthropic PBC (États-Unis). Aucune donnée d'élève ne lui est transmise.

Annexe III — Mesures techniques et organisationnelles

Mesures mises en œuvre par le sous-traitant, décrites telles qu'elles sont en place dans Oléo à la date de ce contrat.

Chiffrement des données au repos

- Noms, prénoms et dates de naissance des élèves, et mémos, chiffrés en AES-256-GCM, un vecteur d'initialisation tiré au hasard pour chaque valeur : deux prénoms identiques ne se ressemblent pas dans la base, et toute altération du fichier est détectée au déchiffrement.
- Les annotations et les remarques libres ne sont pas chiffrées ; elles sont rattachées à des élèves dont le nom l'est.
- Clé de 256 bits propre à chaque environnement (production, préproduction, développement), conservée sur le serveur hors de la base, et jamais copiée avec les sauvegardes : une copie de la base qui sortirait du serveur ne nomme aucun élève.
- Après chaque chiffrement de données existantes, compactage de la base (VACUUM), pour qu'aucune ancienne valeur en clair ne subsiste dans le fichier.

Protection des données pendant la transmission

- Application servie uniquement en HTTPS ; toute adresse en HTTP est redirigée.
- Cookie de session réservé au HTTPS, inaccessible aux scripts de la page et non transmis aux requêtes venues d'autres sites ; les appels à l'application dont l'origine déclarée n'est pas la sienne sont refusés.

Identification, autorisation et cloisonnement

- Mots de passe jamais enregistrés : seule une empreinte bcrypt est conservée.
- Limitation du nombre de tentatives : 10 connexions en 5 minutes, 5 inscriptions par heure, 6 envois de code par courriel en 30 minutes et 15 vérifications de code en 15 minutes ; ces codes expirent au bout de 15 minutes.
- Comptes cloisonnés : chaque requête est restreinte aux données du compte connecté. Un banc d'essai automatisé interroge chaque route de l'application avec les identifiants d'un autre compte et vérifie qu'aucune donnée ne passe.
- Aucun espace parents ni élèves : seul l'enseignant titulaire du compte accède à ses classes.

Disponibilité, sauvegarde et restauration

- Sauvegarde quotidienne de la base, prise de façon cohérente pendant le fonctionnement, relue et vérifiée (intégrité, tables, lignes) avant d'être conservée ; une sauvegarde défaillante ne remplace jamais les précédentes.
- Copie quotidienne des sauvegardes hors du serveur, sur un ordinateur de l'éditeur, en France, hors de tout service de stockage en ligne.
- Procédure de restauration documentée, avec vérification de la base restaurée avant remise en service.

Tests, évolutions et configuration

- Bancs d'essai automatisés (cloisonnement, chiffrement, conservation, migrations) exécutés sur chaque demande de fusion avant toute mise en production.
- Évolutions de la base appliquées dans une transaction unique, avec comptage et vérification des données avant et après : une vérification qui échoue annule l'évolution entière.
- Préproduction distincte, protégée par mot de passe, avant chaque mise en production.

Minimisation, conservation limitée et responsabilité

- Effacement automatique des données des élèves au terme de la durée fixée à l'annexe II, sans réglage possible pour la prolonger.
- Mesure de l'usage réduite aux jours d'ouverture et au type de modification, sans contenu ni heure, effacée au bout de treize mois.
- Aucune publicité, aucun traceur, aucune revente ni cession de données.
- Accès au serveur réservé à l'éditeur. Le tableau de suivi de l'éditeur n'affiche jamais un élève, un nom d'élève ni une annotation ; son accès exige de ressaisir le mot de passe, dure 30 minutes et est limité à 5 essais par quart d'heure.

Assistance au responsable du traitement

- L'enseignant consulte, corrige et supprime à tout moment, depuis l'application, les données de ses élèves.
- FLUOW répond aux demandes de l'établissement (exercice des droits, analyse d'impact, audit) par le formulaire de contact ou à contact@fluow-design.fr, et lui fournit les éléments techniques nécessaires.

Annexe IV — Liste des sous-traitants ultérieurs

Liste convenue au titre de la clause 7.7, point a) (autorisation écrite générale). Tout ajout ou remplacement est notifié par écrit au responsable du traitement trente jours à l'avance.

1. Nom	O2SWITCH, société par actions simplifiée, SIREN 510 909 807
Adresse	Chemin des Pardiaux, 63000 Clermont-Ferrand
Personne de contact	Service client d'o2switch · 04 44 44 60 40
Description du traitement	Hébergement de l'application, de sa base de données et de ses sauvegardes sur le serveur ; envoi des courriels de connexion. Données stockées en France. Seul sous-traitant ultérieur, il n'a pas à délimiter ses responsabilités avec un autre.