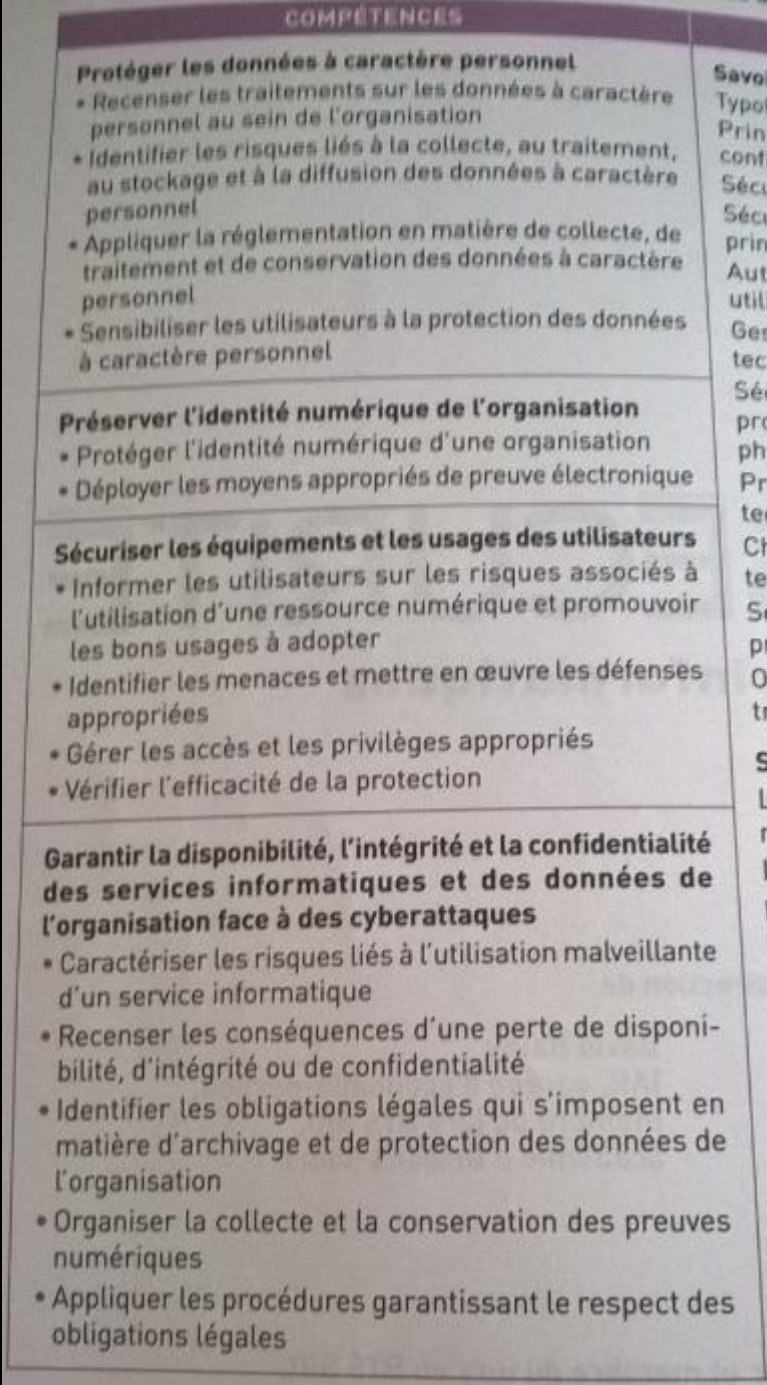


Compétences	
• Objectif principal	Mettre en place le RGPD à travers le projet de l'association WEBCOURSES
• Objectifs intermédiaires	•
• Outils utilisés	• Internet • Base documentaire disponible sur Ecole directe • Le projet WEBCOURSES + Running Hightech + Java Stock
Mode de travail	• Seuls ou en groupe selon leur préférence
Mode d'évaluation	• Validation des missions au fil de l'eau, en direct, sur une base personnelle et selon son rythme jusqu'à la fin de chaque semestre

	• Chaque compte-rendu est à poser dans le PFC • Épreuve E6 certificative
--	---

Sommaire

Présentation du projet RGPD	4
Running Hightech	4
Présentation de l'équipe de RUNNING HIGHTECH.....	4
Les données gérées par RUNNING HIGHTECH.....	5
La collecte des données par RUNNING HIGHTECH.....	5
Relation WEBCOURSES / RUNNING HIGHTECH.....	5
Présentation de l'équipe de l'Association WEBCOURSES	6
Les données gérées par WENCOURSES.....	6
La collecte des données par WENCOURSES.....	7
Présentation de Javastocks	7
La collecte des données par Javastocks.....	7
Relation Jeux d'esprits / RUNNING HIGHTECH	8
Présentation de Jeux d'esprits	8
Les données gérées par Jeux d'esprits.....	8
La collecte des données par Jeux d'esprits.....	8
Relation Catamarans / RUNNING HIGHTECH.....	9
Présentation de Catamarans	9
Les données gérées par Catamarans.....	9
La collecte des données par Catamarans.....	9
Relation Aventures Alpines / RUNNING HIGHTECH.....	9
Présentation d'Aventures alpines	10
Les données gérées par Aventures Alpines.....	10
La collecte des données par Aventures Alpines.....	10
RGPD Prise de connaissance du projet.....	11
Mission 1 Analyse des contextes.....	11
RGPD Outils de proactivité pour sécuriser les traitements	13
Mission 1 Créer une PIA	13
RGPD partie légale des sites.....	19
Mission 1 Rajouter les mentions légales générales.....	19
Mission 2 Créer la page de politique de confidentialité.....	21
Mission 3 Gérer l'utilisation des cookies.....	23
Mission 4 Créer la charte cookies	25
Mission 5 Créer la page de consentement du traitement des données à caractère personnel.....	26
Mission 6 Gérer l'obligation du respect du droit à l'image, du droit d'auteur, de la réglementation de liberté d'expression lors de la publication de contenus	27
RGPD Les courriers pour agir.....	28
Mission 1 Créer un courrier de demande de droit d'accès électronique, de demande de rectification des données incomplètes, de demande de rectification des données inexactes, de demande de droit à l'oubli	28
RGPD Le droit à l'information.....	31
Mission 1 Créer une charte d'utilisation des bonnes pratiques informatiques (présentation à faire aux autres sections de BTS)	31

Mission 2 Construire une formation de sensibilisation du personnel au respect du RGPD (présentation à faire aux autres sections de BTS).....	33
RGPD Outils de proactivité pour sécuriser les traitements	35
Mission 2 Le registre des traitements	35
RGPD la gestion des contrats	37
Mission 1 Analyser un contrat d'hébergement puis un contrat de sous-traitance entre running hightech et l'association WEBCOURSES	37
Mission 2 Compléter votre contrat de sous-traitance afin d'y intégrer les SLA (les accords de niveau de service) négociés entre Web Course et Running Hightech	53

Présentation du projet RGPD

Running Hightech

La RUNNING HIGHTECH est une structure indépendante, financée par des donateurs, le Conseil Régional de Paris dont l'administration est déléguée au Comité Régional Olympique et Sportif de Paris (CROSP).

Elle a pour mission de fournir des espaces et des services aux différentes associations sportives régionales et à d'autres structures hébergées.

Comme d'autres structures cérébrales comme Jeux d'esprit ou de structures sportives comme Aventures Alpines ou Catamarans, la RUNNING HIGHTECH a accueilli récemment un nouveau membre : l'association WEBCOURSES. Cette dernière souhaite pouvoir profiter de l'infrastructure et des services offerts par cette dernière.

Afin de pouvoir gérer au mieux les différentes demandes en lien avec le RGPD, RUNNING HIGHTECH désire mettre en place une base de données regroupant tous ces aspects afin de répondre à la demande de ses clients. Ceci a été validé par les membres de la direction du SI.

Présentation de l'équipe de RUNNING HIGHTECH

La société, basée à Levallois-Perret, au 12 Boulevard de Levallois Prol, Elle dispose de locaux disposés sur deux bâtiments de 3000m² de 5 étages.

RUNNING HIGHTECH est découpé en plusieurs services : RH, comptabilité, informatique, commercial et relation clients et composé d'une cinquantaine de salariés, dont 10 commerciaux,

Le service informatique est composé de 10 personnes, dirigé par Mme Chaussetoi Socky, responsable des traitements, joignable au 01-45-56-12-12, adresse mail : chaussetoi.runninghightech@gmail.com et son MDP : Running@Hightech

Elle est secondée par Mme Loyal, la DPO du service, en lien avec la RH et le comité de direction, joignable au 01-45-56-12-13, adresse mail loyal.runninghightech@gmail.com. C'est aussi la personne dédiée à l'exercice des droits des personnes concernées.

Les autres collaborateurs sont 5 techniciens de maintenance et 3 administrateurs réseaux confirmés.

Le capital social de Running Hightech est de 1.000.000 euros et son SIREN est le SIREN **123 111 941 00057 (numéro de siren suivi du NIC et le tout donne le SIRET) , RCS PARIS B 123 111 941 (B pour société commerciale, suivi du siren)**

Nomenclature APE : 6202A - Conseil en systèmes et logiciels informatiques

Numéro de TVA : **FR 32 123111941 (FR + clé de contrôle "32" + numéro SIREN)**

Son site internet est <https://www.webrunning.fr>

Directeur de publication et propriétaire : Mme chaussetoi

Développeurs : équipe informatique de développement de running hightech

Afin de répondre aux attentes de ses clients, la RUNNING HIGHTECH met en place une infrastructure basée sur des serveurs Windows 2022, comprenant :

- La gestion des comptes et des droits utilisateurs ainsi que le déploiement de stratégies de groupe
- La gestion des sites
- La réplication
- Le service de gestion des noms de domaine
- La distribution des adresses dynamiques
- Les contrôles des accès dynamiques
- La gestion des services de gestion des droits
- La mise en place d'un espace sécurisé et en particulier un serveur mandataire
- Gérer la répartition de charge et la répartition réseau
- Gérer la haute disponibilité

Elle se dote également d'un serveur de supervision de type Nagios, d'un serveur Ubuntu sur lequel elle installera DNS et DHCP.

Les données gérées par RUNNING HIGHTECH

- Les différents sites des associations
- Le service de gestion des noms de domaine
- La gestion des services de gestion des droits
- La mise en place d'un espace sécurisé et en particulier un serveur mandataire

La collecte des données par RUNNING HIGHTECH

- Les adresses IP en lien avec le plan d'adressage et celui des clients
- Les noms de domaines
- Pour chaque membre interne de la société :
 - Nom
 - Prénom
 - Téléphone
 - Adresse mail
- Le mot de passe de connexion aux différents services d'habilitations de la société
- Toutes les informations de logs relatives à la base de données Active Directory
- Toutes les informations de logs relatives au serveur de messagerie

Relation WEBCOURSES / RUNNING HIGHTECH

WEBCOURSES et RUNNING HIGHTECH ont signé un contrat de sous-traitance afin de pouvoir héberger la base de données WEBCOURSES chez Running Hightech, mais aussi tous les traitements relatifs à la bonne marche de l'association. Elle s'assure ainsi d'une sécurité renforcée et de l'appui d'un professionnel informatique.

L'association WEBCOURSES s'inscrit dans le contexte RUNNING HIGHTECH, qui a pour mission de fournir des espaces et des services à différents clients et à d'autres structures hébergées.

Présentation de l'association WEBCOURSES

Elle fédère des événements principalement tournés vers la course : vélo, natation, course à pied...

Elle gère environ un million de membres dont dix mille professionnels.

Elle accueille des compétiteurs/compétitrices amateurs comme professionnels, de France ou d'Europe. Ces derniers ont le droit de s'engager sur une course à partir de 10 ans.

L'association est située au 45 rue des mathurins à Paris dans le 8^{ème}.

Le capital social de webcourses est de 1.230.000 euros et son SIREN est le **123 568 941 00056**.

Pas de RCS ou de RM car c'est une association de la loi 1901.

Nomenclature APE : 94.99Z organisation fonctionnant par adhésion volontaire

Numéro de TVA : **aucun car les activités à caractère éducatif, culturel, sportif ou social** dans le cadre d'un service rendu par une association à ses membres a une gestion désintéressée.

Son site internet est <https://www.webcourses.fr>

Directeur de publication, développeur et propriétaire : adminDB

Présentation de l'équipe de l'Association WEBCOURSES

Principalement composés de volontaires, l'association emploie 5 salariés à temps plein :

- Une personne responsable de l'événementiel, joignable au 01-45-45-45-13, adresse mail evènement@webcourses.fr
- Une commerciale responsable du lien avec les clubs sportifs, joignable au 01-45-45-45-14, adresse mail commercial@webcourses.fr
- Une personne responsable de la gestion des inscriptions, joignable au 01-45-45-45-15, adresse mail inscriptions@webcourses.fr
- Le gestionnaire de la base de données webcourses est M.adminDB,, joignable au 01-45-45-45-16, adresse mail adminDB@webcourses.fr
- Le gestionnaire de la base de données Javasotck est M.Stoker, joignable au 01-45-45-45-12, adresse mail stoker@webcourses.fr . C'est lui qui est en charge de la réservation et de l'approvisionnement des produits textiles, boissons et denrées sèches lors des différentes courses.

Les données gérées par WENCOURSES

Sur la page qui sommes-nous, une photo de l'équipe au complet de l'association ou des deux fondateurs est affichée.

On y trouve l'adresse et plan d'accès de l'association ainsi que le numéro de téléphone et adresse mail de l'association.

Sur le calendrier événementiel, on retrouve toutes les informations en lien avec un événement sportif à savoir les informations sur les championnats, les manifestations, les catégories d'épreuve, les épreuves, les parcours et les catégories d'âge.

La page informations club donne des informations générales sur la vie d'un club, le nombre d'adhérents pour l'année en cours et l'historique du classement du club (année / classement)
Sur la page personnelle ses courses / ses classements, on trouve pour les courses :

- Le nom,
- Le prénom,
- La date à laquelle un membre a participé à une course,
- Le type épreuve
- Le temps réalisé

et pour le classement :

- L'année
- Le rang
- Les points obtenus
- Le nombre de victoires
- Le nombre de défaites

La collecte des données par WENCOURSES

Afin de pouvoir gérer la base de données at l'application appliwebcourses, les données suivantes sont collectées par WEBCOURSES pour chaque membre de l'association :

- Nom
- Prénom
- Rue
- CP
- Ville
- Téléphone
- Pseudo
- Adresse mail
- Le mot de passe
- Le sexe
- La date de naissance
- Numéro de licence
- Le certificat médical d'aptitude à jour
- Le temps réalisé pour une course
- La taille du maillot

Présentation de Javastocks

Javastocks est la BDD permettant à webcourses de pouvoir gérer les préparatifs d'un évènement. Il sert à gérer les stocks de nourriture, boisson et tee-shirts pour un coureur sur une épreuve donnée. Le site gère aussi le réapprovisionnement des produits.

La collecte des données par Javastocks

- Le nom produit, son type, la taille, la couleur, le volume, le poids de nourriture
- Pour l'épreuve, le nom, le lieu, la date de début et de fin,
- Le type d'épreuve

- Le nom et le prénom du coureur
- Numéro de réservation, date de réservation, quantité du produit désirée

Relation Jeux d'esprits / RUNNING HIGHTECH

Jeux d'esprits et RUNNING HIGHTECH ont signé un contrat de sous-traitance afin de pouvoir héberger la base de données de Jeux d'esprits chez Running Hightech, mais aussi tous les traitements relatifs à la bonne marche de la société. Elle s'assure ainsi d'une sécurité renforcée et de l'appui d'un professionnel informatique.

Présentation de Jeux d'esprits

Jeux d'esprit vise à attirer un public en quête de stratégie, de réflexion, aussi bien adulte que jeunes. Afin de gérer les jeux de la plateforme Jeux d'Esprit, le maître des jeux doit gérer et développer différents jeux pour permettre à des jeunes ou des adultes de s'amuser ou bien de s'affronter entre eux. Elle est gérée par le maître des jeux, employé à temps plein.

Le capital social de Jeux d'esprits est de 300.000 euros et son SIREN est le SIREN **123 333 941 00056 (numéro de siren suivi du NIC et le tout donne le SIRET) , RCS PARIS B 123 333 941 (B pour société commerciale, suivi du siren)**

Nomenclature APE : **4791B**

Numéro de TVA : **FR 32 123333941 (FR + clé de contrôle "32" + numéro SIREN)**

Son site internet est <https://www.jeuxdesprits.fr>

Directeur de publication et propriétaire : M. Maître des Jeux

Développeurs : M. Maître des Jeux

Les données gérées par Jeux d'esprits

Les caractéristiques principales sont la gestion statistique en lien avec les jeux : nombre de joueur, les connexions effectuées, les nombres de parties jouées

La collecte des données par Jeux d'esprits

- Libellé du niveau
- Le statut de la partie
- Le score, le temps de la partie, nombre de parties jouées
- Le nom, l'adresse mail et l'avatar du joueur
- Le nom du jeu et le nombre de joueur associé à ce jeu
- Le type de jeux

Relation Catamarans / RUNNING HIGHTECH

Catamarans et RUNNING HIGHTECH ont signé un contrat de sous-traitance afin de pouvoir héberger la base de données de Catamarans chez Running Hightech, mais aussi tous les traitements relatifs à la bonne marche de la société. Elle s'assure ainsi d'une sécurité renforcée et de l'appui d'un professionnel informatique.

Présentation de Catamarans

Catamarans est une plateforme en ligne conçue spécialement pour les amoureux du sport de mer en catamarans, de loisirs ou sportifs. Que vous soyez farniente ou un battant, permet aux amoureux de grands espaces de parcourir le monde à leur rythme.

Le capital social de Catamarans est de 250.000 euros et son SIREN est le SIREN **123 444 941 00056 (numéro de siren suivi du NIC et le tout donne le SIRET)** , RCS PARIS B 123 444 941 (B pour société commerciale, suivi du siren)

Nomenclature APE : **4791B**

Numéro de TVA : **FR 32 123444941 (FR + clé de contrôle "32" + numéro SIREN)**

Son site internet est <https://www.catamarans.fr>

Directeur de publication et propriétaire : M. Du Bateau

Développeurs : M. Du Bateau

Les données gérées par Catamarans

Les caractéristiques principales sont la gestion de l'occupation d'un catamaran par un équipage et des passagers.

La collecte des données par Catamarans

- Nom, type bateau, longueur, largeur, hauteur, tirant d'eau, la vitesse
- La catégorie de catamaran
- Pour le loisir, la voile, la coque roto moulée
- Pour le sportif, foc, dérives flottantes, la grand-voile
- Pour les passagers, le nom, prénom, tel et email
- Le nom et le prénom d'un membre d'équipage

Relation Aventures Alpines / RUNNING HIGHTECH

Aventures Alpines et RUNNING HIGHTECH ont signé un contrat de sous-traitance afin de pouvoir héberger la base de données d'Aventures Alpines chez Running Hightech, mais aussi tous les traitements relatifs à la bonne marche de la société. Elle s'assure ainsi d'une sécurité renforcée et de l'appui d'un professionnel informatique.

La société Aventures Alpines s'inscrit dans le contexte RUNNING HIGHTECH, qui a pour mission de fournir des espaces et des services à différents clients et à d'autres structures hébergées.

Présentation d'Aventures alpines

Aventures Alpines est une plateforme en ligne conçue spécialement pour les amoureux du sport de montagne et de l'exploration en altitude. Que vous soyez un grimpeur passionné, un randonneur tranquille ou simplement fasciné par la beauté majestueuse des montagnes, Aventures Alpines vous offre un espace pour vous informer, vous inspirer et partager vos expériences.

Le capital social d'Aventures Alpines de 455.000 euros et son SIREN est le SIREN **123 222 941 00056 (numéro de siren suivi du NIC et le tout donne le SIRET) , RCS PARIS B 123 222 941 (B pour société commerciale, suivi du siren)**

Nomenclature APE : **4791B**

Numéro de TVA : **FR 32 123222941 (FR + clé de contrôle "32" + numéro SIREN)**

Son site internet est <https://www.aventuresalpines.fr>

Directeur de publication et propriétaire : M.Alpin

Développeurs : équipe informatique de développement d'Aventures Alpines

Les données gérées par Aventures Alpines

Les caractéristiques principales sont la découverte des sports de montagne, tel que le ski, l'escalade ou la randonnée, des informations en format blogs, articles ou vidéos, une partie réservation de prestation ainsi que la notation des prestations par les clients.

La collecte des données par Aventures Alpines

- Vidéo
- Articles
- Liens de blog
- La région pour la randonnée
- Lieu de départ
- Lieu d'arrivée
- Nombre de km
- Praticable été comme hivers
- Pour le ski, le nom du domaine
- Pour l'escalade, le site, le niveau de difficulté et le temps d'ascension
- Pour le client, nom, prénom et adresse
- Date de début et fin de réservation
- Le nombre de personnes concernées
- Prix de la réservation
- Nom de la prestation

RGPD Prise de connaissance du projet

Mission 1 Analyse des contextes

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions
Objectifs	Rédiger le registre des traitements relatif à la partie application WEBCOURSES
Objectifs intermédiaires	Réinvestir les notions de cours en développement / CEJMA / réseau / CEJM
Pré-requis	Cours CEJMA / cours cybersécurité
Évaluation	Compte-rendu est à poser dans votre PFC Épreuves certificatives E4, E5 et E6

Votre mission

A partir des informations se trouvant dans la présentation du contexte, il vous est demandé :

Les acteurs

1. Lister l'ensemble des acteurs mentionnés internes et externes chez Running Hightech et WEBCOURSES à l'aide d'un tableau

Nom de la société	Acteur interne	Acteur externe

Les traitements des données à caractère personnel

2. Recenser les traitements des données à caractère personnel chez Running Hightech et WEBCOURSES

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité	

Les données à caractère personnel

3. **Définir** la notion de données à caractère personnel
4. **Recenser** à l'aide d'un tableau, les données à caractère personnel, DCP et DCPS qui transitent chez Running Hightech et WEBCOURSES.

Nom de la société	Catégories de données personnelles concernées	Données à caractère personnel ou DCP	Données à caractère personnel sensible ou DCPS
	État civil, identité, données d'identification, images...		
	Vie personnelle (habitudes de vie, situation familiale, etc.)		
	Données de connexion (adresse IP, logs, etc.)		

Les responsables des données à caractère personnel

5. **Définir** la notion de responsables de traitements à caractère personnel
6. **Recenser** à l'aide d'un tableau, les responsables de traitements à caractère personnel pour Running Hightech et WEBCOURSES.

Nom de la société	Responsable traitements	Tâche de cette personne

Les logiciels

Avec l'aide du paragraphe aide documentaire ci-dessous :

- **Définir** les notions de logiciels libres / propriétaires utilisés
- **Expliquer** les droits des utilisateurs par rapport aux licences
- **Détailler** les tarifs associés aux licences quand cela est nécessaire
- **Identifier** les clauses d'audit
- **Etablir** un diagnostic des différents types de logiciels utilisés chez WEBCOURSES et Running Hightech à partir des informations que vous avez étudié dans la partie 1 de cette mission, des informations que vous détenez sur les projets WEBCOURSES et Running Hightech

Aide documentaire

- **Les différents types de logiciel** : <https://www.techno-science.net/glossaire-definition/Logiciel-propretaire.html>
- **Le droit d'auteur et les logiciels** : <https://www.legalstart.fr/fiches-pratiques/proteger-une-creation/protection-logiciel/>
- **Contrat de licence** : <https://droit-finances.commentcamarche.com/faq/23680-contrat-de-licence-definition>

RGPD Outils de proactivité pour sécuriser les traitements

Mission 1 Créer une PIA

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions	
Evaluation		Production d'écrit DST E6

Objectif principal

Créer une PIA

Objectifs intermédiaires

- **Réinvestir** les notions de cours de géolocalisation

Outils nécessaires

Le logiciel de la CNIL pour créer une PIA ou EIVP étude d'impact sur la vie privée
<https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>

Pré-requis

- Cours Bloc3 cybersécurité tronc commun Mme Peyrataud / cloud / semestre 2 / cybersécurité / géolocalisation

Énoncé du problème

Il s'agit d'explicitier, dans le document PIA et de manière technique, les tâches de traitement de données décrites par l'énoncé suivant :

La société PrivateRun réalise un logiciel d'acquisition, stockage et traitement de données de running, issues d'un dispositif de type "montre connectée", pour le compte de l'association webcourses.

L'architecture considérée est la suivante :

1. La montre connectée (e.g. Android) appartenant à l'utilisateur, client de la société PrivateRun. L'utilisateur a installé un logiciel propriétaire de PrivateRun qui permet de récupérer des informations sur la géolocalisation de la personne la portant (position, vitesse et estampille, c'est-à-dire date et heure) et de les stocker en local sur la montre, mais également de pouvoir les uploader sur un serveur de PrivateRun.
2. Des serveurs (ou cloud) loués par PrivateRun à la société SuperCloudProvider, sur lesquels la société PrivateRun a installé un logiciel permettant d'effectuer des traitements sur les données uploadées par les utilisateurs sur ce cloud, et de les présenter sur un site web hébergé sur le même cloud. Le site web contient une partie

privée, contenant les données de toutes les trajectoires d'un utilisateur, accessible via des login et mot de passe, et une partie publique avec des données qui sont disponibles à tout le monde, sans login.

Les traitements des données sont donc, pour chaque utilisateur, d'être capable d'afficher ses positions de géolocalisation datées, de manière privée, et d'afficher des cartes de chaleur, c'est-à-dire les traces de tous les utilisateurs, mais sans indiquer à qui appartient la trace.

La société PrivateRun recueille le consentement des utilisateurs via un formulaire signé de leur part pour le traitement de leurs données : nom, prénom, date de naissance et géolocalisation (stockage sur la montre et les serveurs, et sur leur serveur), en indiquant deux finalités :

- **F1- afficher de manière privée toutes leurs traces et calculer par exemple leur meilleur temps de parcours ;**
- **F2- afficher l'ensemble des traces des coureurs, mais de manière "anonyme", c'est-à-dire sans indiquer le nom et le prénom de la personne à qui appartient la trace.**

Votre mission

- **Créer** la PIA pour la société PrivetaRun à l'aide du logiciel de la CNIL
- Vérifiez que votre PIA remplit les critères suivants :
 - Les éléments importants sont présents.
 - Les descriptions sont cohérentes.
 - Les solutions proposées ne comportent pas d'erreurs et peuvent être mises en œuvre.
 - La validation par le responsable de traitement a été réalisé
 - Vous avez obtenu la cartographie de votre PIA
- **Cartographier** les risques
- **Evaluer** et **commenter** les résultats obtenus
- **Imprimer** le plan d'action proposé
- **Repérer** les changements rendus visibles par la cartographie

Aide Documentaire

Préparation

Télécharger le logiciel de la CNIL pour créer une PIA ou EIVP étude d'impact sur la vie privée : <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>

Ce logiciel est disponible pour Linux, Mac et Windows, et ne pose aucun souci particulier d'installation. La version utilisée ici est la version 2.0.0 (Windows).

Une fois installé et lancé, la page de présentation du logiciel devrait ressembler à ceci :



Page de présentation du logiciel PIA

Si jamais la langue n'est pas le français, il est possible de la modifier en appuyant sur l'icône du globe terrestre en haut à droite de l'écran.

Après avoir cliqué sur "Commencer" vous arrivez sur l'écran de chargement ou sélection d'un projet. Cliquez sur le symbole + à côté de "nouveau PIA".



Nouveau PIA

Remplissez les champs permettant de définir le projet PIA, puis cliquez sur "commencer".

Pia PIA - Privacy Impact Assessment

Edit View Window

Version 2.0.0

pia Analyse d'impact sur la protection des données
privacy impact assessment

ACCUEIL MODÈLES DE PIA EXEMPLE DE PIA Outils

liste Trier

PIA

PIA Montre PrivateRun

Saisie

Votre nom

Évaluation

DPO de PrivateRun

Validation

PDG de Private Run

Modèle

Modèle par défaut

Validation

29/04/2019

Statut

Création 0%

Commencer

Tous les champs doivent être remplis

Description des intervenants dans le PIA

Travail demandé

Votre objectif, au cours de ce PIA, est de remplir les 3 premières parties de ce document (sur la colonne de gauche de la fenêtre), à savoir les parties :

1. **Contexte.**
2. **Principes Fondamentaux.**
3. **Risques.**

Vous pouvez naviguer d'une partie à l'autre en cliquant sur les liens sur la partie gauche de la fenêtre. Dans ce qui suit, nous allons donner quelques précisions sur la manière de remplir ces parties.

La partie **4- Validation** correspond aux commentaires et à la validation par le DPO et du responsable du traitement de votre PIA. Vous allez tenir ce rôle de manière à obtenir la cartographie de cette dernière.

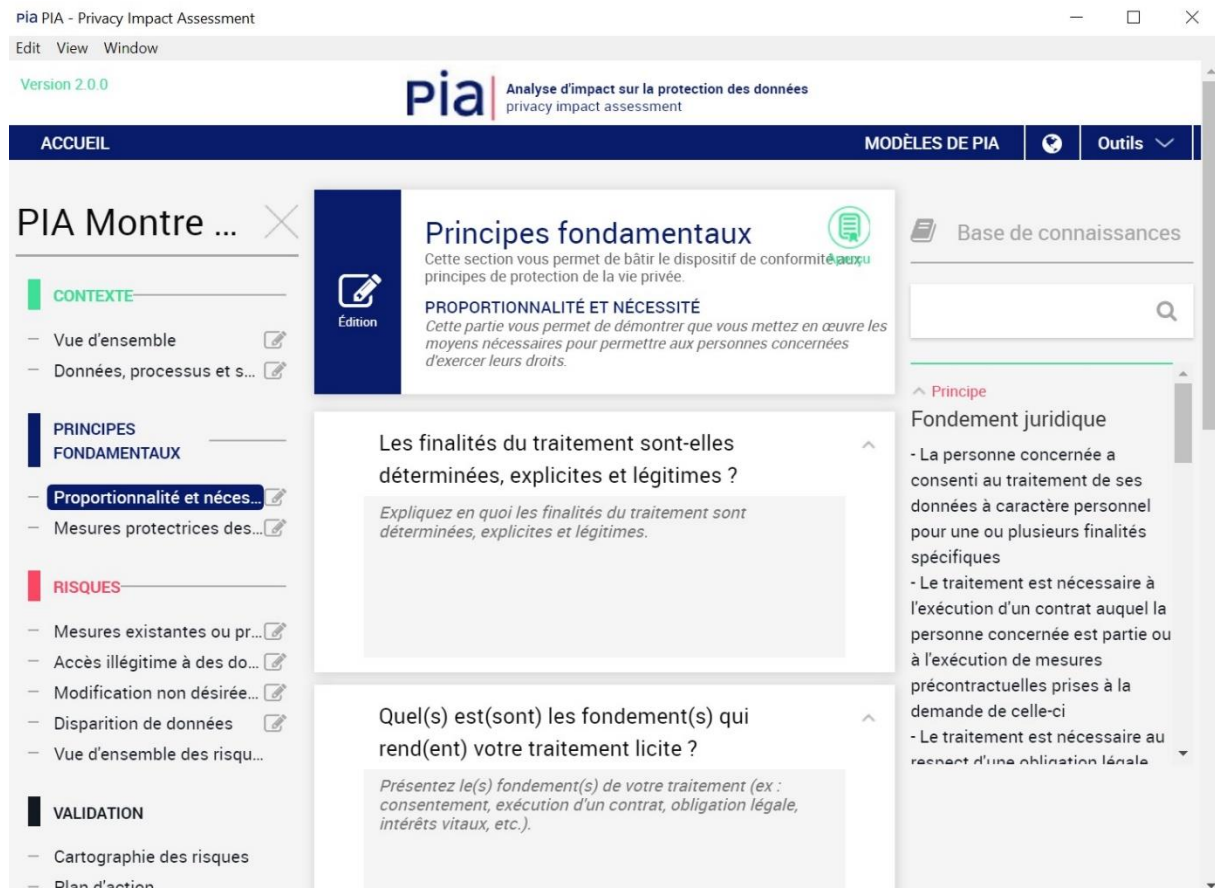
En revenant sur la liste de tous vos projets (en cliquant sur le bouton "**Accueil**" en haut à gauche de la fenêtre), vous pouvez exporter votre projet en **format JSON**, ou importer d'autres projets, toujours dans ce même format.

La partie validation n'est accessible qu'à partir du moment où vous aurez rempli les 3 premières parties de la PIA.

Menu général du logiciel PIA

Le processus à suivre est celui qui est décrit par les trois premières étapes. L'objectif est de décrire de manière claire et succincte les conditions de traitement des données personnelles par l'ensemble de l'application.

Il est important de noter que vous disposez d'indications sur comment remplir chacune des parties dans la colonne droite de l'écran. Chaque concept est défini, et des exemples sont donnés pour comprendre les questions à se poser sur comment remplir chaque champ.



Fondements d'un traitement de données personnelles

Par exemple, pour remplir le champ "*Quel(s) est(sont) le(s) fondement(s) qui rend(ent) votre traitement licite ?*" qui se trouve dans la partie **2- Principes Fondamentaux / Proportionnalité et Nécessité**, il convient d'ouvrir l'onglet "Principe : Fondement juridique". Celui-ci donne la liste de plusieurs raisons qui font que le traitement serait licite. Il s'agit de choisir l'une d'entre elles.

À la question "*Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?*" on pourra consulter l'onglet "Principe : Minimisation des données", et donner des arguments montrant qu'on respecte bien ce principe : ne pas collecter des données qui ne servent à rien.

RGPD partie légale des sites

Mission 1 Rajouter les mentions légales générales

Compétences

Compéter et approfondir toutes les compétences relatives aux différentes missions

Objectif principal

Gérer les mentions légales et les cookies d'un site web

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Un éditeur de texte
- WAMP ou MAMP ou XAMP
- MySql
- PHP

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Votre mission partie 1

- **Lire** le document « Les mentions légales d'un site web - fiche ressource » disponible sur le cloud école directe, dans Bloc3 tronc commun Mme Peyrataud / bloc3 / semestre 2 / projet / RGPD
- **Repérez** les informations nécessaires à la constitution des mentions légales de votre site
- **Utilisez** les générateurs page suivante mis à votre disposition pour créer les mentions légales du site appliwebcourses
- **Prendre** les informations disponibles dans la partie présentation du projet RGPD de ce document et utilisez-les pour remplir les informations nécessaires à WEBCOURSES
- **Rajouter** les mentions légales générales dans le footer de votre site qui doivent être accessibles via un lien afin de ne pas surcharger la page en lecture.

Aide rédactionnelle

- Quelles sont les mentions obligatoires sur un site internet ? <https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228>
- Mentions légales pour les cookies : <https://www.legalplace.fr/guides/mentions-legales-cookies/>

- Cookies et traceurs : comment mettre mon site web en conformité ? : <https://www.cnil.fr/fr/cookies-et-traceurs-comment-mettre-mon-site-web-en-conformite>

Générateurs et modèles de mentions légales

Il existe beaucoup de générateurs de mentions légales de site Internet pour vous permettre de ne rien oublier. Ils sont en général **gratuits**.

Voici une liste de générateurs connus que vous pouvez utiliser :

- SubDelirium : <https://www.subdelirium.com/generateur-de-mentions-legales/#generateur>
- Générateur de mentions légales : <https://www.generateur-de-mentions-legales.com/>
- Générer des mentions légales : <https://www.generer-mentions-legales.com/>

Conseil

Cependant ces générateurs ne remplacent pas les conseils de juristes ou d'avocats spécialisés. Ils répondent néanmoins aux exigences des administrateurs pour la plupart des sites Web si les contenus de ces sites ne sont pas liés à des cadres juridiques spécifiques ou étendus.

Les diverses présences sur le web ne sont pas les seules concernées par l'obligation de présenter les mentions légales. Tout employé qui envoie des emails au nom de l'entreprise, et qui rédige ainsi une lettre commerciale est concerné. En effet, ces emails doivent également contenir les mentions légales ou mentions obligatoires correspondantes.

Mission 2 Créer la page de politique de confidentialité

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions
Evaluation	Production d'écrit DST E6

Objectif principal

Créer la page de politique de confidentialité + charte cookies d'un site web

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Un éditeur de texte
- WAMP ou MAMP ou XAMP
- MySql
- PHP

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Votre mission

- **Lire** le document Construire sa page de politique de confidentialité - fiche ressource disponible sur le cloud école directe, dans Bloc3 tronc commun Mme Peyrataud / bloc3 / semestre 2 / projet / RGPD
- **Repérez** les informations nécessaires à la constitution des politiques de confidentialités de votre site
- **Utilisez** les générateurs ci-dessous mis à votre disposition pour créer les politiques de confidentialité du site appliwebcourses
- **Prendre** les informations disponibles dans la partie présentation du projet RGPD de ce document et utilisez-les pour remplir les informations nécessaires à WEBCOURSES
- **Rajouter** la page de politiques de confidentialité dans le footer de votre site qui doit être accessible via un lien afin de ne pas surcharger la page en lecture.

Aide rédactionnelle

- La politique de confidentialité sur Internet : <https://www.ionos.fr/digitalguide/sites-internet/droit-dinternet/politique-de-confidentialite-sur-internet/>

Générateurs de politiques de confidentialité

- <https://www.tlmr-avocats.com/e-services/generateur-de-politique-de-confidentialite-conforme-rgpd/>
- <https://www.politiquedeconfidentialite.ca/>
- <https://www.privacypolicies.com/fr/>

Mission 3 Gérer l'utilisation des cookies

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions
Evaluation	Production d'écrit DST E6

Objectif principal

Gérer les mentions légales et les cookies d'un site web

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Un éditeur de texte
- WAMP ou MAMP ou XAMP
- MySql
- PHP

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Votre mission partie 1

Ouvrir MAMP, WAMP, XAMP

Aller sur le cloud école directe, dans Bloc3 tronc commun Mme Peyrataud / bloc3 / semestre 2 / projet / RGPD pour créer et charger la base de données RGPD à l'aide des documents création_bdd_rgpd.txt et chargement_bdd_rgpd.txt

Votre mission partie 2

Créer un formulaire PHP, à partir de votre site web, capable de gérer les cookies (tout accepter / tout refuser / choix personnel avec nécessaire, performance, fonctionnalité fortement recommandée pour que le site fonctionne, marketing, autres) et de les stocker dans la table consentement cookie de votre base de données RGPD.

Informations utiles

-- Création de la table consentement des cookies

```
DROP TABLE IF EXISTS consentement_cookie;
```

```
CREATE TABLE consentement_cookie(  
  cok_id INT AUTO_INCREMENT NOT NULL,  
  cok_type_consentement CHAR(1),
```

```
cok_necessaire BOOLEAN,  
cok_performance BOOLEAN,  
cok_fonctionnalite BOOLEAN,  
cok_marketing BOOLEAN,  
cok_autres BOOLEAN,  
adh_id INT NOT NULL,  
PRIMARY KEY(cok_id),  
FOREIGN KEY(adh_id) REFERENCES adherents(adh_id)  
)ENGINE=InnoDB;
```

- Si la personne a cliqué sur tout accepter, la valeur des champs dans la table sont à 1.
- Si la personne a cliqué sur tout refuser, la valeur des champs dans la table sont à 0
- Si la personne a cliqué sur personnaliser, la valeur des champs dans la table dépendent de ce qui a été coché

Mission 4 Créer la charte cookies

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions
Evaluation	Production d'écrit DST E6

Objectif principal

Créer la page de politique de confidentialité + charte cookies d'un site web

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Machine srvweb.ova
- virtualbox

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Votre mission

- **Lire** le document Chap 3.3 - CHARTE SUR LES COOKIES du site Le ROUTARD - Fiche ressource disponible sur le cloud école directe, dans sio1 tronc commun / bloc3 / semestre 2 / cejma / TD
- **Repérez** les informations nécessaires à la charte cookies de votre site
- **Prendre** les informations disponibles dans la partie présentation du projet RGPD de ce document et utilisez-les pour remplir les informations nécessaires à WEBCOURSES
- **Rajouter** la charte cookies pour webcourses. Cette dernière est à rajouter dans le footer **de votre site** et doit être accessible via un lien afin de ne pas surcharger la page en lecture.

Aide rédactionnelle

- La politique de confidentialité sur Internet : <https://www.ionos.fr/digitalguide/sites-internet/droit-dinternet/politique-de-confidentialite-sur-internet/>
- Mentions légales pour les cookies : <https://www.legalplace.fr/guides/mentions-legales-cookies/>

Mission 5 Créer la page de consentement du traitement des données à caractère personnel

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions
Evaluation	Production d'écrit DST E6

Objectif principal

Créer la page du consentement du traitement des données à caractère personnel d'un site web

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau

Outils nécessaires

- Machine srvweb.ova
- virtualbox

Pré-requis

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Votre mission

- **Utilisez** le lien ci-après <https://www.cnil.fr/fr/exemples-de-formulaire-de-collecte-de-donnees-caractere-personnel>
- **Prendre** les informations disponibles dans la partie présentation du projet RGPD de ce document et utilisez-les pour remplir les informations nécessaires à WEBCOURSES
- **Créer** la page de consentement du traitement des données à caractère personnel
- **Rajouter** le consentement en format PDF téléchargeable pouvant être envoyé par adresse mail ou par courrier

Aide rédactionnelle

- RGPD : QUELS CHANTIERS PRIORITAIRES POUR VOTRE SITE WEB ?
Demander le consentement : <https://www.eanet.fr/web-marketing/rgpd-quelles-consequences-site-web>
- Formulaire Google droit à l'oubli : adresse et mode d'emploi : <https://droit-finances.commentcamarche.com/faq/39882-formulaire-google-droit-a-l-oubli-adresse-et-mode-d-emploi>

Mission 6 Gérer l'obligation du respect du droit à l'image, du droit d'auteur, de la réglementation de liberté d'expression lors de la publication de contenus

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions
Evaluation	Production d'écrit DST E6

Objectif principal

Construire une formation de sensibilisation du personnel au respect du RGPD

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Machine srvweb.ova
- virtualbox

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité) / CEJM

Votre mission

- **Rajouter** une nouvelle page sur le site appliwebcourses en y intégrant des photos de coureurs, de courses, des articles afin de mettre en œuvre le respect du droit à l'image, du droit d'auteur, la réglementation de liberté d'expression (pour cela gérer des commentaires).

RGPD Les courriers pour agir

Mission 1 Créer un courrier de demande de droit d'accès électronique, de demande de rectification des données incomplètes, de demande de rectification des données inexactes, de demande de droit à l'oubli

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions
Evaluation	Production d'écrit DST E6

Objectif principal

Créer une demande de droit d'accès électronique

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau

Outils nécessaires

- Machine srvweb.ova
- virtualbox

Pré-requis

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Votre mission

Demande de droit d'accès cas 1

Monsieur Hernandez Perez Rocca souhaite faire une demande de droit d'accès auprès de webcourses. Aidez-le à rédiger son courrier

- **Utilisez** le lien suivant : <https://www.cnil.fr/fr/modele/courrier/exercer-son-droit-dacces>
- **Remplir** une demande de droit d'accès électronique auprès du responsable de traitement de webcourses.
- **Déposez** cette demande dans la base de données de RGPD sur la table courrier_rgpd en la personne de monsieur Hernandez Perez Rocca, gérée via un formulaire

Réponse du responsable de traitement ou du DPO concernant la demande de droit d'accès de monsieur Hernandez Perez Rocca

→ La demande acceptée

- Rédigez la réponse que vous donnez dans un délai de 1 mois maximum selon l'Art12.3 RGPD et donnez une copie gratuite de l'art.15 du RGPD
- ➔ Gérer la base de données RGPD en conséquence

Demande de droit d'accès cas 2

Monsieur Hernandez Sanchez Bartoli envoie une demande de droit d'accès auprès de WEBCOURSES pour la 15^{ème} fois en un mois.

- **Déposez** les demandes dans la base de données de RGPD sur la table courrier_rgpd en la personne de monsieur Hernandez Sanchez Bartoli, gérée via un formulaire.

Réponse du responsable de traitement ou du DPO concernant la demande de droit d'accès de monsieur Hernandez Sanchez Bartoli

- La demande est refusée car rentre dans un cadre systématique
- Rédigez la réponse à la demande contestée
- ➔ Gérer la base de données RGPD en conséquence

Demande de rectification des données incomplètes

Madame Barnes Edith souhaite faire une demande de rectification des données incomplètes auprès de WEBCOURSES. En effet, cette dernière, habitant dans un immeuble, s'est aperçue que son adresse était incomplète car il manquait le numéro de bâtiment, la porte d'entrée du bâtiment, l'étage et son numéro de porte. Aidez-la à rédiger son courrier.

- **Utilisez** le lien suivant : <https://www.cnil.fr/fr/modele/courrier/rectifier-des-donnees-incomplètes>
- **Remplir** une demande de droit de rectification de données incomplètes (art.16 RGPD)
- **Déposez** cette demande dans la base de données RGPD sur la table courrier_rgpd en la personne de madame Barnes Edith, gérée via un formulaire

Réponse du responsable de traitement ou du DPO concernant la demande de rectification des données incomplètes de madame Barnes Edith

- La demande est acceptée
- Rédigez la réponse à la demande de données incomplètes
- ➔ Gérer la base de données RGPD en conséquence (correction de l'adresse, vous prendrez un screen avant et après)

Demande de rectification des données inexacts

Madame Chercheuse Lina souhaite faire une demande de rectification des données inexacts auprès de WEBCOURSES. En effet, cette dernière s'est aperçue que son adresse n'était pas la bonne car elle vient de déménager. Aidez-la à rédiger son courrier.

- **Utilisez** le lien suivant : <https://www.cnil.fr/fr/le-droit-de-rectification-corriger-vos-informations>
- **Remplir** une demande de droit de rectification de données inexacts (art.16 RGPD)

- **Déposez** cette demande dans la base de données RGPD sur la table courrier_rgpd en la personne de madame Chercheuse Lina, gérée via un formulaire

Réponse du responsable de traitement ou du DPO concernant la demande de rectification des données inexactes de madame Chercheuse Lina

- La demande est acceptée
- Rédigez la réponse à la demande de données inexactes
- ➔ Gérer la base de données RGPD en conséquence (correction de l'adresse, vous prendrez un screen avant et après)

Application des connaissances du cours

- **Expliquer** ce qui se passe en cas de non réponse de la part du responsable de traitement sur une demande de droit de rectification
- **Documenter** votre explication en utilisant le lien suivant de la CNIL
<https://www.cnil.fr/fr/webform/adresser-une-plainte>

Demande de droit à l'oubli

Monsieur Jumbo Charles est sur le point de décrocher un nouveau poste à responsabilité mais une photo de lui portant une couronne de roi mais en tenu d'Adam, suite à une victoire de course à pied, figure sur le site appliwebcourses. Ayant peur de montrer une mauvaise image de lui envers ses futurs recruteurs, ce dernier souhaite faire une demande de droit à l'oubli. Aidez-le à rédiger son courrier.

- **Utilisez** le formulaire ci-dessous pour créer une demande de droit à l'oubli **MAIS NE PAS FAIRE ENVOYER. Utilisez** un document WORD à **transformer en PDF** pour le poser sur votre site
- **Déposez** cette demande dans la base de données RGPD sur la table courrier_rgpd en la personne de monsieur Jumbo Charles, gérée via un formulaire

Formulaire de demande droit à l'oubli : <https://reportcontent.google.com/forms/rtbf?hl=fr>

Réponse du responsable de traitement ou du DPO concernant la demande de rectification des données inexactes de monsieur Jumbo Charles

- La demande est acceptée
- Rédigez la réponse à la demande du droit à l'oubli
- ➔ Gérer la base de données RGPD en conséquence ainsi que le site appliwebcourses (enlever la photo, vous prendrez un screen avant et après)

Intégrez le tout dans la base de données RGPD

Utilisez le fichier creation_bdd_rgpd.txt et chargement_bdd_rgpd.txt se trouvant dans l'espace de travail Bloc3 cybersécurité tronc commun mme Peyrataud / cloud / Projets / RGPD pour créer votre BDD RGPD

RGPD Le droit à l'information

Mission 1 Créer une charte d'utilisation des bonnes pratiques informatiques (présentation à faire aux autres sections de BTS)

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions	
Evaluation		Production d'écrit DST E6

Objectif principal

Créer une charte d'utilisation des bonnes pratiques informatiques

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Claroline
- Word ou office
- HTML/CSS/JS

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Votre mission

- **Créer** une charte d'utilisation des bonnes pratiques informatiques (mettre en veille, changer son mdp, ne pas l'écrire, etc,,,) dans le format qui vous semble le plus pertinent

Les attendus de la charte

1. Titre : rappel des bonnes pratiques
2. Sécuriser l'accès à son compte
3. La gestion du courrier électronique
 - 3.1. Messagerie privée
 - 3.2. Contrôle de l'usage
4. Utilisation d'Internet
 - 4.1. Internet à des fins privées
 - 4.2. Contrôle de l'usage

5. Pare feu
6. Sauvegardes
7. La signature de l'entreprise et celle de l'employé

Aide documentaire

Sur le site, <https://www.coover.fr/modeles/gestion-entreprise/exemple-charte-informatique> ,
ouvrir notre modèle de charte informatique pour vous aidez

Mission 2 Construire une formation de sensibilisation du personnel au respect du RGPD (présentation à faire aux autres sections de BTS)

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions	
Evaluation		Production d'écrit DST E6

Objectif principal

Construire une formation de sensibilisation du personnel au respect du RGPD

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Claroline
- Word ou office
- HTML/CSS/JS

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Votre mission

- **Construire** une formation de sensibilisation du personnel au respect du RGPD au sein de WEBCOURSES et Running Hightec

Les attendus de la formation (2h de présentation)

- PowerPoint animé
- Intégrer des vidéos (la vidéo de la hack academy sur le https et celui de choupinette via les réseaux sociaux)
- La notion de données personnelle, de donnée personnelle sensible
- Comment les données personnelles sont-elles collectées, conservées et traitées ? Quelles données sont collectées par l'entreprise ?
- Comment sont utilisées les données ?
- Combien de temps sont-elles conservées ?
- Les droits du client 6 Quelles sont les obligations du client ?
- Comment l'entreprise assure la sécurité des données ? ...
- Monter concrètement ce que ceci peut donner (pirater deux postes : un en changeant le fond d'écran avec une image de hacking, l'autre en changeant le mot de passe par pirate)

- Donner les points importants du RGPD (protection, mot de passe, mise à jour, mettre en veille, changer son mdp, ne pas l'écrire, etc,,,))
- Ne pas faire confiance aveuglément
- Expliquer les sanctions encourues

Aide documentaire

https://www.bureaupcr.fr/Charte_des_bonnes_pratiques_RGPD_site_internet.pdf

RGPD Outils de proactivité pour sécuriser les traitements

Mission 2 Le registre des traitements

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions	
Evaluation		Production d'écrit DST E6

Objectif principal

Rédiger le registre des traitements d'un des projets développés : aventures alpines, webcourses, Catamarans, Jeux d'esprit, Javastocks, webrunning, running hightech

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

Le registre des traitements

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Contenu d'un registre des activités de traitement

Le RGPD propose une liste de questions simples servant de fil conducteur...

- Quelle est la personne responsable des traitements ? Préciser son nom et ses coordonnées, ainsi que celles du représentant, du DPO et des sous-traitants, s'il y en a.
- Dans quel but les données à caractère personnel sont-elles collectées ? Notifier toutes les finalités de façon très précise (constitution d'un fichier du personnel, d'une liste de fournisseurs, etc.)
- Quelle sont les catégories de personnes visées par les traitements (employés, clients, adhérents, patients, etc.) ? Et quelles sont les catégories de données récoltées (noms, coordonnées, photos d'identité, numéros de téléphone, CV, bulletins de salaires, plaques d'immatriculation, habitudes de consommation, adresses IP, etc.) ? Ne pas oublier de spécifier les données sensibles.
- Où seront localisées les données ? Quelle sera leur destination finale et qui va les gérer ? Lister tous les destinataires.

Projet RGPD transversal avec tous les autres projets

- Y-a-t-il des transferts hors de l'Union européenne ? Si oui, préciser les noms des destinataires et leur pays d'origine.
- Quelle sera la durée de conservation des données ? Préciser leur délai d'effacement, lequel peut différer d'une catégorie à l'autre.

Travail à faire

1. Constituer un groupe
2. Choisir un projet selon votre spécialité

SLAM	Nom du projet	SISR	Nom du projet
	Aventures alpines		Webrunning
	Webcourses		Running hightech
	Catamarans		
	Jeux d'esprit		
	Javastocks		

3. A partir des informations collectées dans les différents projets (se reporter à la présentation du contexte au début du document), remplir le registre des traitements associé
→ fichier excel nommé registre_traitement_base_de_travail.xls disponible le cloud école
directe dans Bloc3 tronc commun Mme Peyrataud / semestre 2 / Projet / RGPD

RGPD la gestion des contrats

Mission 1 Analyser un contrat d'hébergement puis un contrat de sous-traitance entre running hightech et l'association WEBCOURSES

Compétences	Compéter et approfondir toutes les compétences relatives aux différentes missions	
Evaluation		Production d'écrit DST E6

Objectif principal

Etablir un contrat d'hébergement puis de sous-traitance entre running hightech et l'association WEBCOURSES

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Word ou office

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Contexte

Dans un premier temps, l'association WEBCOURSES souhaite établir un contrat d'hébergement avec Running Hightech. Pour se faire, une ébauche a déjà été réalisée entre les deux partis¹ que vous trouverez ci-dessous.

Votre mission

Compléter le contrat d'hébergement à partir du document joint.

¹ Exemple venant de <https://creation-site-internet.ooreka.fr/ebibliotheque/voir/254413/contrat-d-hebergement-d-un-site-internet>

Contrat d'hébergement d'un site internet

Entre les soussignés :

[Nom de la société hébergeur]

[Adresse et siège social] [Pays]

Immatriculée au registre du commerce et des sociétés sous le numéro d'immatriculation [numéro] représentée en la personne de [Nom et Prénom de la personne] en sa qualité de [fonction de la personne dans la société].

[Adresse de courrier électronique]

[Téléphone]

Ci-après désigné comme « l'Hébergeur »,

Et

[Nom de la société client]

[Adresse et siège social] [Pays]

Immatriculée au registre du commerce et des sociétés sous le numéro d'immatriculation [numéro] représentée en la personne de [Nom et Prénom de la personne] en sa qualité de [fonction de la personne dans la société].

[Adresse de courrier électronique]

[Téléphone]

Ci-après désigné comme « le Client ».

Les deux parties ont convenu ce qui suit :

ARTICLE 1 : Objet

Le présent contrat a pour objet l'encadrement juridique des obligations incombant à chacune des parties.

Le contrat confie à la société [Nom de la société], l'hébergement du site internet [Nom du site internet] de [Nom du client] moyennant rémunération.

ARTICLE 2 : Obligations de l'Hébergeur

L'Hébergeur s'engage à héberger sur son serveur le site internet du Client. Il s'oblige à fournir une prestation de qualité.

Selon le cas :

- L'Hébergeur procédera à un hébergement dit « mutualisé » : le Client partagera le serveur avec d'autres clients du prestataire. Le service d'hébergement web vérifiera la mise en place et le bon fonctionnement de l'hébergement après inscription du Client au service.
- L'Hébergeur procédera à un hébergement dit « dédié » : le Client louera et utilisera le serveur à titre exclusif. Le Client aura la possibilité d'utiliser toutes les ressources disponibles.
- L'Hébergeur procédera à un hébergement dit « gratuit » : l'hébergement est gratuit en contrepartie d'une publicité insérée dans le site internet du Client.

ARTICLE 3 : Déclaration des sites internet

L'Hébergeur se verra déléguer par le présent contrat la déclaration des sites internet, en particulier auprès de la Commission nationale de l'informatique et des libertés (CNIL).

L'Hébergeur est tenu d'informer régulièrement le Client de l'avancée des procédures relatives à la déclaration des sites internet.

Éventuellement :

- Le dépôt du nom de domaine sera effectué par l'Hébergeur. L'Hébergeur informera régulièrement le Client de l'avancée de la procédure.

ARTICLE 4 : Obligation du Client

Le Client s'engage au paiement de la prestation d'hébergement dans les délais mentionnés à l'article 5 du présent contrat.

ARTICLE 5 : Prix

La prestation d'hébergement sera facturée au Client à hauteur de [montant en euros] €.

Selon le cas :

- Le Client s'acquitte du paiement à l'hébergement définitif du site internet au plus tard le [date]
- Le Client procède à un paiement forfaitaire du prix à savoir :
 - le [date], premier versement d'un montant de [montant en euros] € ;
 - le [date], deuxième versement d'un montant de [montant en euros] € ;
 - le [date], troisième versement d'un montant de [montant en euros] €, etc.

ARTICLE 6 : Modalités de paiement

Selon le cas :

- Le virement est à réaliser sur le compte [coordonnées bancaires].
- Le chèque est à transmettre à l'ordre de [Ordre].

ARTICLE 7 : Responsabilité limitée

L'Hébergeur met en œuvre tous les moyens nécessaires pour exécuter la prestation d'hébergement.

L'obligation étant de moyens, l'Hébergeur ne peut être tenu pour responsable en cas d'absence de résultat.

ARTICLE 8 : Propriété intellectuelle

Le présent contrat n'opère pas de transfert de propriété des droits intellectuels relatifs aux éléments du site internet vers l'Hébergeur. Le Client jouit seul de la propriété des droits rattachés au site internet.

ARTICLE 9 : Contrefaçon

Toute contrefaçon concernant le site internet en lui-même ou l'un des éléments du site internet, devra faire l'objet d'une communication par l'une des parties à l'autre dès lors qu'elle en a eu connaissance.

ARTICLE 10 : Durée

Le présent contrat est conclu à compter de la signature des parties et ce pour durée de [date]. Le contrat prendra fin le [date].

Éventuellement :

ARTICLE 11 : Confidentialité du contenu

- L'Hébergeur s'oblige à la confidentialité des informations relatives aux clients et aux partenaires de [Nom du client].
- Cela comprend : [Détailer les informations protégées]

ARTICLE 12 : Sécurité du contenu

La sécurité des données et du site internet est assurée par l'Hébergeur.

La sauvegarde des données est effectuée par l'Hébergeur à une fréquence de [fréquence].

L'Hébergeur effectue une étendue de sauvegarde des données de [étendue].

L'hébergeur utilise pour les sauvegardes [le / les] support(s) [indiquer le ou les supports].

ARTICLE 13 : Suspension du contrat

Le présent contrat peut être suspendu par chacune des parties en cas [de violation des obligations contractuelles / en cas de mise à disposition de contenu illicite, etc.]

Un avertissement sans effet aura pour conséquence une suspension du contrat.

Selon le cas :

- Le contrat sera suspendu pour une durée de [durée].
- Le contrat fera l'objet d'une suspension limitée à la régularisation de la situation défailante.

ARTICLE 14 : Résiliation

Chacune des parties pourra procéder à la résiliation du présent contrat en cas de manquement aux obligations stipulées.

La partie défaillante recevra par courrier recommandé avec accusé de réception une mise en demeure de s'exécuter. En cas d'inexécution, la partie ayant respecté son engagement contractuel pourra sans délai résilier le présent contrat.

Le solde des sommes dues sera établi au prorata de la prestation exécutée.

ARTICLE 15 : Changement de prestataire

En fin de contrat, le Client peut procéder à un changement de prestataire, même concurrent de l'Hébergeur initial.

À cette fin, le transfert de l'hébergement du site internet du Client devra impérativement s'opérer au plus tard le [date].

Les données devront être restituées par l'hébergeur avant le [date] et récupérées par le Client avant le [date].

ARTICLE 16 : Droit applicable et juridiction compétente

La législation [française / autre législation] s'applique au présent contrat.

En cas d'absence de résolution amiable d'un litige né entre les parties, seuls les tribunaux du ressort de la Cour d'appel de [Ville] sont compétents.

Fait en deux exemplaires, le [date] à [Ville].

Signature précédée de la mention « lu et approuvé » :

[Signature de l'Hébergeur] [Signature du Client]

Contexte

Dans un second temps, l'association webcourses souhaiterait aller plus loin dans les relations avec Running Hightec. Pour cela, l'association envisage de passer un contrat de sous-traitance avec running hightech.

Votre mission

- **Télécharger** le contrat de sous-traitance proposé à l'adresse suivante
<https://www.habitatpresto.com/pro/conseils/pratiques/modele-contrat-sous-traitance>
- **Compléter** ce contrat

Contexte

Pour aller encore plus loin, l'association Webcourses veut intégrer des clauses à ce contrat de sous-traitance.

Pour **encadrer cette relation** entre les deux parties en cas de litige, voici les éléments et clauses à faire figurer dans l'accord :

1. L'objet du contrat
2. La description des travaux confiés au sous-traitant
3. La durée d'exécution des travaux, cadence des commandes, délais de livraison
4. Les sanctions du non-respect des cadences et des délais
5. Les délais de paiement et/ou pénalités de retard
6. La clause d'indexation ou clause de renégociation en cas d'évolution des conditions économiques compromettant l'équilibre du contrat
7. Le prix de la prestation
8. Les modalités de modification du contrat
9. Le contrôle et réception des prestations
10. Les garanties
11. La confidentialité
12. La propriété intellectuelle / savoir-faire
13. Le régime des modèles et outillages spécifiques (assurances, rétention, etc.)
14. La clause sur le travail dissimulé
15. La date de conclusion, date d'effet du contrat
16. Le tribunal compétent et droit applicable

Votre mission

- A l'aide du document ci-dessous, **intégrer** les clauses de sous-traitance au contrat entre webcourses et running hightech.

Sous-traitance : Exemple de clauses²

[...], situé à [...] et représenté par [...]

(ci-après, « **le responsable de traitement** »)

d'une part,

ET

[...], situé à [...] et représenté par [...]

(ci-après, « **le sous-traitant** »)

d'autre part,

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « **le règlement européen sur la protection des données** »).

II. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) [...].

La nature des opérations réalisées sur les données est [...].

La ou les finalité(s) du traitement sont [...].

Les données à caractère personnel traitées sont [...].

Les catégories de personnes concernées sont [...].

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes [...].

III. Durée du contrat

Le présent contrat entre en vigueur à compter du [...] pour une durée de [...].

² <https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses>

IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. Traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance
2. Traiter les données **conformément aux instructions documentées** du responsable de traitement figurant en annexe du présent contrat. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en **informe immédiatement** le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public
3. **Garantir la confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat
4. Veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :
 - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
 - Reçoivent la formation nécessaire en matière de protection des données à caractère personnel
5. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception** et de **protection des données par défaut**
6. **Sous-traitance**

Choisir l'une des deux options :

Option A (autorisation générale)

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minium de [...] à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Option B (autorisation spécifique)

Le sous-traitant est autorisé à faire appel à l'entité [...] (ci-après, le « sous-traitant ultérieur ») pour mener les activités de traitement suivantes : [...]

En cas de recrutement d'autres sous-traitants ultérieurs, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique du responsable de traitement.

Quelle que soit l'option (autorisation générale ou spécifique)

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

7. Droit d'information des personnes concernées

Choisir l'une des deux options :

Option A

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Option B

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

8. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Choisir l'une des deux options :

Option A

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à [...] (*indiquer un contact au sein du responsable de traitement*).

Option B

Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

9. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de [...] heures après en avoir pris connaissance et par le moyen suivant [...]. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Option possible

Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- La description de la nature de la violation de 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 ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de données à caractère personnel ;
- La description des mesures prises ou 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.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- La description de la nature de la violation de 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 ;

- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou 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.

10. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

[Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres

- *La pseudonymisation et le chiffrement des données à caractère personnel*
- *Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*
- *Les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;*
- *Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement]*

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues par *[code de conduite, certification]*.

[Dans la mesure où l'article 32 du règlement européen sur la protection des données prévoit que la mise en œuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en œuvre]

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :

Au choix des parties :

- Détruire toutes les données à caractère personnel ou bien

- À renvoyer toutes les données à caractère personnel au responsable de traitement ou bien
- À renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

13. Délégué à la protection des données

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son délégué à la protection des données**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données

14. Registre des catégories d'activités de traitement

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- Les catégories de traitements effectués pour le compte du responsable du traitement ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - La pseudonymisation et le chiffrement des données à caractère personnel ;
 - Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
 - Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15. Documentation

Le sous-traitant met à la disposition du responsable de traitement **la documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

V. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. Fournir au sous-traitant les données visées au II des présentes clauses
2. Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
3. Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant
4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant

Mission 2 Compléter votre contrat de sous-traitance afin d'y intégrer les SLA (les accords de niveau de service) négociés entre Web Course et Running Hightech

Compétences	Compléter et approfondir toutes les compétences relatives aux différentes missions
Evaluation	Production d'écrit DST E6

Objectif principal

Compléter le contrat de sous-traitance afin d'y intégrer les SLA (les accords de niveau de service) négociés entre WEBCOURSES et Running Hightech

Objectifs intermédiaires

- **Réinvestir** les notions de cours en développement / CEJMA / réseau / CEJM

Outils nécessaires

- Word ou office

Pré-requis

- Cours de développement / CEJMA / réseau (support et cybersécurité)

Votre mission

Partie 1

- A partir de la vidéo <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203473-sla-service-level-agreement-definition-translation/> **Expliquer** le rôle des SLA (les accords de niveau de service)

Partie 2

- **Compléter** votre contrat de sous-traitance afin d'y intégrer les SLA (les accords de niveau de service) négociés entre Web Course et Running Hightech à l'aide du paragraphe aide rédactionnelle ci-dessous

Aide rédactionnelle

SLA des SaaS : ce que doivent inclure les contrats : <https://www.lemagit.fr/conseil/SLA-des-SaaS-ce-que-doivent-inclure-les-accords>

Gartner : 9 critères pour établir un contrat de SLA en interne
<https://www.lemagit.fr/conseil/Gartner-9-criteres-pour-etablir-un-contrat-de-SLA-en-interne/>