**Sécuriser un local technique**

Sommaire

[Introduction 1](#_Toc120617537)

[L’emplacement et conception principal de la salle 1](#_Toc120617538)

[Sécuriser l’accès à la salle informatique 3](#_Toc120617539)

[La climatisation 3](#_Toc120617540)

[Protection anti-incendie 5](#_Toc120617541)

[Armoires et câblage 5](#_Toc120617542)

[L’électricité dans la salle 6](#_Toc120617543)

[Protection des données 8](#_Toc120617544)

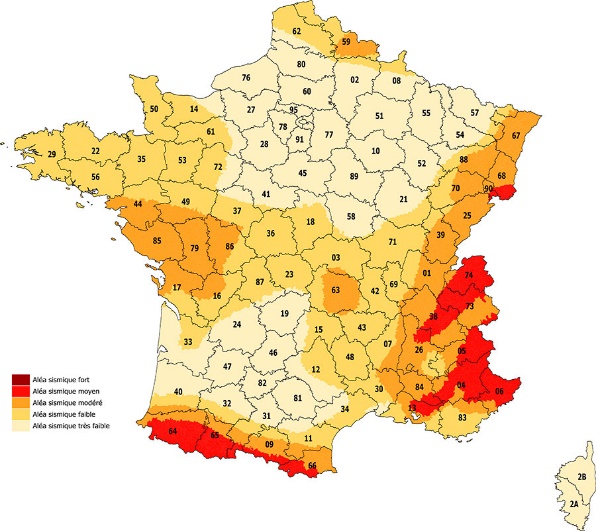
# Introduction

La salle informatique est le cœur de l’entreprise, elle permet en effet la connexion entre toutes les salles, entre les postes de travails et les serveurs. Avant de choisir les différentes solutions de sécurité de la salle en elle-même, il est primordial de bien choisir l’emplacement de cette dernière.

# L’emplacement et conception principal de la salle

Elle doit :

* Se trouver dans un bâtiment aux normes antisismique surtout si le local se situe dans une zone de sismicité élevée (identifiables sur une carte semblable à celle ci-dessous)



* Être sans fenêtres
* Sur une dalle en béton (pour éviter les

inondations)

* Être située au rez-de-chaussée pour éviter

Les escalier (pratique pour l’installation de

matériel) ou au premier étage si le bâtiment est situé dans une zone d’innondation

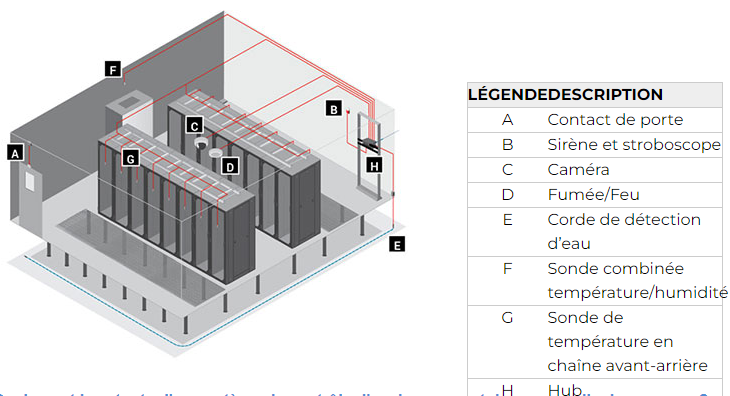
* Avoir des murs en béton recouvert d’une

Peinture empêchant la propagation de feux

* Mise en place d’un faux-plancher
  + Utilise l’espace entre les deux planchers pour fournir de l’air conditionné
  + Permettre de modifier aisément l’agencement de la salle
  + Protège les câbles de connexion et les prises électriques
  + Il doit être construit avec des matériaux à l’épreuve ou résistant au feu
* Être hermétique et ignifugée du sol au plafond
* Voisine de salles elles-mêmes sûres
* Dans la mesure du possible, protéger la salle d’un

Revêtement en aluminium (**cage de faraday**) bloquant les ondes (afin de la protéger **contre tous dispositifs d’espionnage à distance**), il faudrait donc préconiser l’utilisation de **téléphones filaires** dans la salle.

* Utilisation de la **technologie PoE** (power of Ethernet) permettant aux switch d’alimenter les téléphones en électricité par Ethernet
* Mise en place d’une surveillance de l’environnement par l’intermédiaire d’un hub et de sondes et capteurs reliés à celui-ci.



Le hub permet de centraliser toutes les données recueillies par les sondes et diffuser des alertes au personnel lorsque les données son anormales via le réseau.

3 éléments principaux la composent :

* + Unité de base ou hub
  + Sondes ou capteurs
  + Connexion et intégration réseau du hub

# Sécuriser l’accès à la salle informatique

Il faut en premier lieu **installer une porte adéquate** permettant de **rendre la salle hermétique à l’extérieur** notamment aux gaz d’extinction d’incendies ainsi qu’au incendies de s’échapper dans le reste du bâtiment : elle doit donc être **ignifugée**.

L’accès à la salle doit être uniquement possible par l’intermédiaire d’**une carte magnétique** permettant de **gérer les autorisations** (seules les personnes habilitées peuvent entrer) cela permet également de surveiller les allées et venues du personnel (journalisation).

Alternative peu couteuse pouvant être utilisé en complément de l’accès par carte

Un carnet peut également être ajouté dans la salle dans lequel chaque intervenant doit noter son nom, heure d’entrée/sortie et raison de sa présence.

D’autres systèmes sont à mettre en place afin de sécuriser l’accès à une salle informatique tels que :

* Un système de vidéosurveillance 24h/24 et 7j/7
* Détecteur de mouvements
* Vérification des antécédents du personnel
* Processus de mise à jour des droits d’accès
* Sécurité virtuelle (serveurs virtuels accessibles uniquement via un logiciel de virtualisation avec le profil administrateur)

# La climatisation



Etant donné que la salle informatique est totalement hermétique à l’extérieur, il est obligatoire de mettre en place un système de climatisation :

* Pour le **maintien d’une température et un taux d’humidité correcte** pour le bon fonctionnement du matériel informatique (21 degré et un taux d’humidité compris entre 30% et 50 %)
* Pour le confort du personnel devant intervenir dans la pièce.

Exemple des datacenters de Google Cloud et Oracle victimes d’interruptions temporaire de leurs services du aux fortes chaleurs cet été au Royaume-Uni.

<https://www.lemondeinformatique.fr/actualites/lire-grande-bretagne-le-pic-de-chaleur-fait-tomber-les-datacenters-de-google-cloud-et-oracle-87442.html>

L’installation

* Protéger la sortie de climatisation par une grill pour empêcher une quelconque intrusion
* Prévoir **plusieurs climatiseurs** pouvant prendre le relais en cas de panne ou ne maintenance (une alarme peut être déclenchée en cas d’interruption involontaire)
* Opter pour un **système de refroidissement adiabatique** : humidification contrôlée de l’air de la salle pour la refroidir.



Refroidissement adiabatique

Remarque : le refroidissement adiabatique **n’est pas soumis au règlement ICPE** (installations classées pour la protection de l’environnement), il est **peu exigeant en eau** et permet de réaliser des **économies d’énergies**.

* Equiper la salle de thermomètre et hygromètres

# Protection anti-incendie



L’atténuation du risque d’incendies est la partie la plus simple et la moins coûteuse mais aussi la plus souvent ignorée. Voici les bonnes pratiques et techniques pour prévenir et stopper les incendies :

* **Ne jamais stocker de matériaux inflammables** dans la salle (poubelle, papiers, cartons)
* Installation de **détecteurs de fumée, de flamme, de chaleurs** au plafond et au sol reliés à une alarme :
  + **Sonore** indiquant aux personnes présentes dans la salle qu’il faut évacuer
  + **Visuelle** dans le couloir interdisant aux personnes à l’extérieur de rentrer dans la salle.

Les incendies ne pouvant pas être éteint à l’eau (cela pourrait endommager le matériel épargné par les flammes), un **gaz** ayant comme propriété d’**absorber l’oxygène** (permettant de stopper les flammes) est diffusé dans la salle. Il faudrait donc :

* Ajouter un détecteur permettant de prévenir les personnes à l’extérieur quand le gaz est évacué pour qu’ils puissent savoir quand pouvoir rentrer à nouveau
* Mettre à disposition des masques à oxygène au cas où la ou les personne(s) présente(s) dans la salle n’aient pas eu le temps de sortir avant l’arrivée du gaz

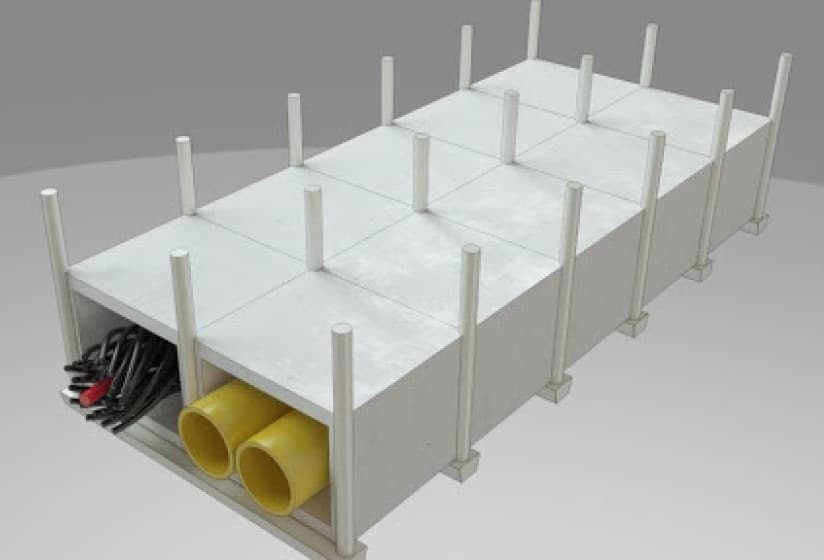
# Armoires et câblage

La salle permettant la connexion serveur-postes, de câbles vont bien devoir sortir de la salle.

* Isoler les chemins de câbles avec :
  + Un calfeutrage coupe-feu.

* + Un encoffrement coupe-feu (bonus esthétique)



* **Numéroter chaque câble et chaque point de connexion** dans les armoires où les baies de brassage (permet d’organiser le câblage et de gagner du temps lors des résolutions de pannes) sur des étiquettes ignifugées

Les prérequis pour les baies de brassage :

* Les placer au milieu de la salle ou alors de façon à **pouvoir accéder à tous les côtés de l’armoire** sans efforts
* Les raccorder à la terre en plus d’un **équipement parafoudre ou parasurtenseur** pour dévier tous afflux électrique anormal vers la terre pour éviter de les endommager

# L’électricité dans la salle

* La lumière doit être assurée par les tubes néon (ou autre **gaz inerte**) afin d’éviter les accidents
* Un **éclairage de secours** est à prévoir
* Toutes les prises de la salle doivent être aussi **raccordées à la terre** et à un fusible du panneau électrique.
* **Le nombre de prise doit être suffisant pour pouvoir installer tous les équipements nécessaires** de façon à ce que chaque câble d’alimentation ait sa propre prise afin d’éviter de devoir installer des multiprises
* Installation obligatoire d’un **onduleur**

**Le rôle de l’onduleur**



* Appareil **régulateur du courant** transformant l’électricité qu’il reçoit en entrée (quel que soit son intensité) en courant « propre » c’est-à-dire **sans fluctuation et permanant** avec lequel il alimente l’équipement auquel il est rattaché (il assure une continuité du courant).
* En cas de coupure de courant générale, **les batteries de l’onduleur prennent le relais**, la durée de vie des batteries dépendent du nombre d’appareils présents dans la salle. Elle doit être suffisante pour que le personnel accrédité accède à la salle et puissent arrêter tous les appareils.
* Il fait l’objet d’une maintenance annuelle et les batteries doivent être vérifiées et changées régulièrement.

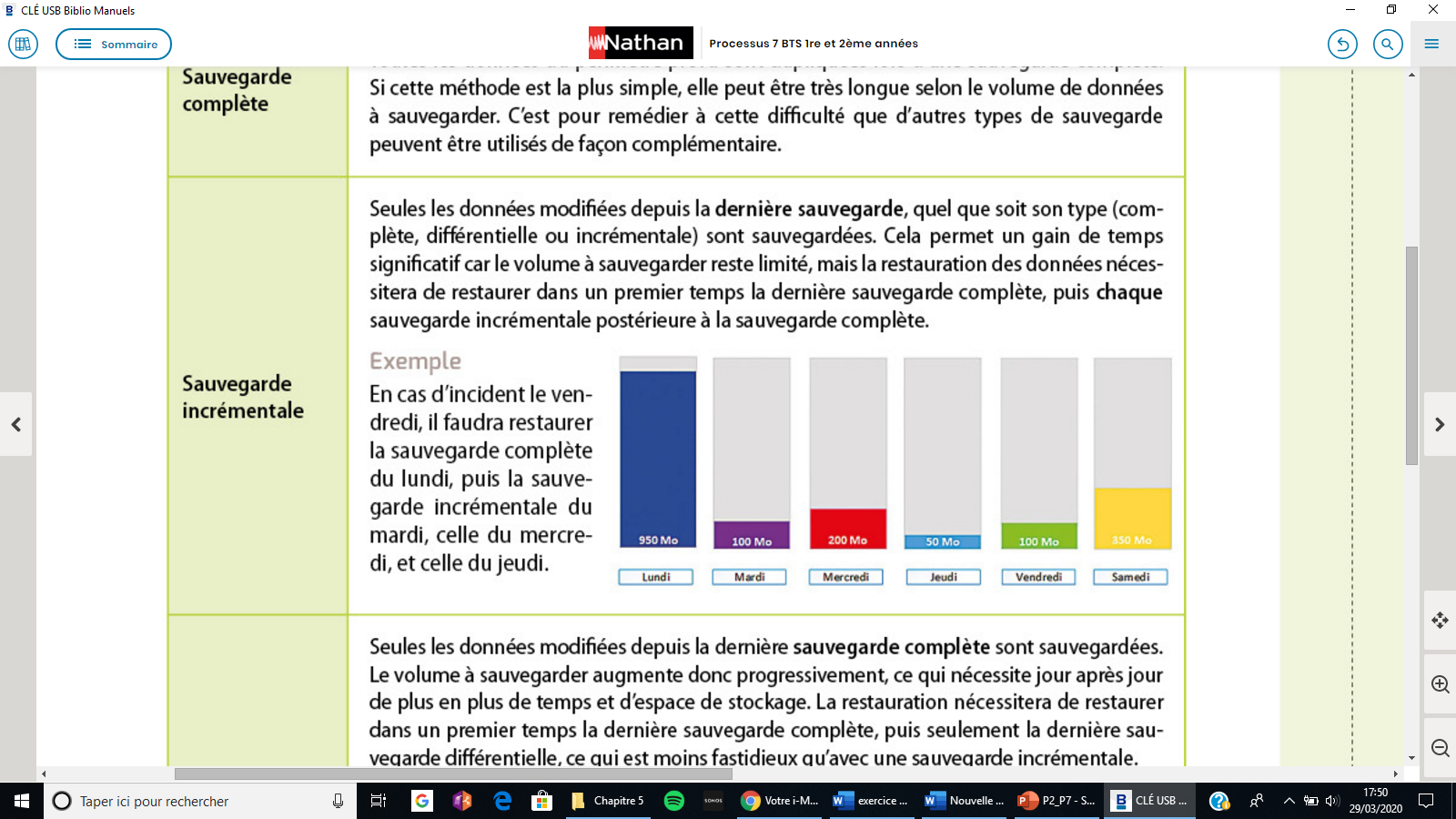
**Le générateur**

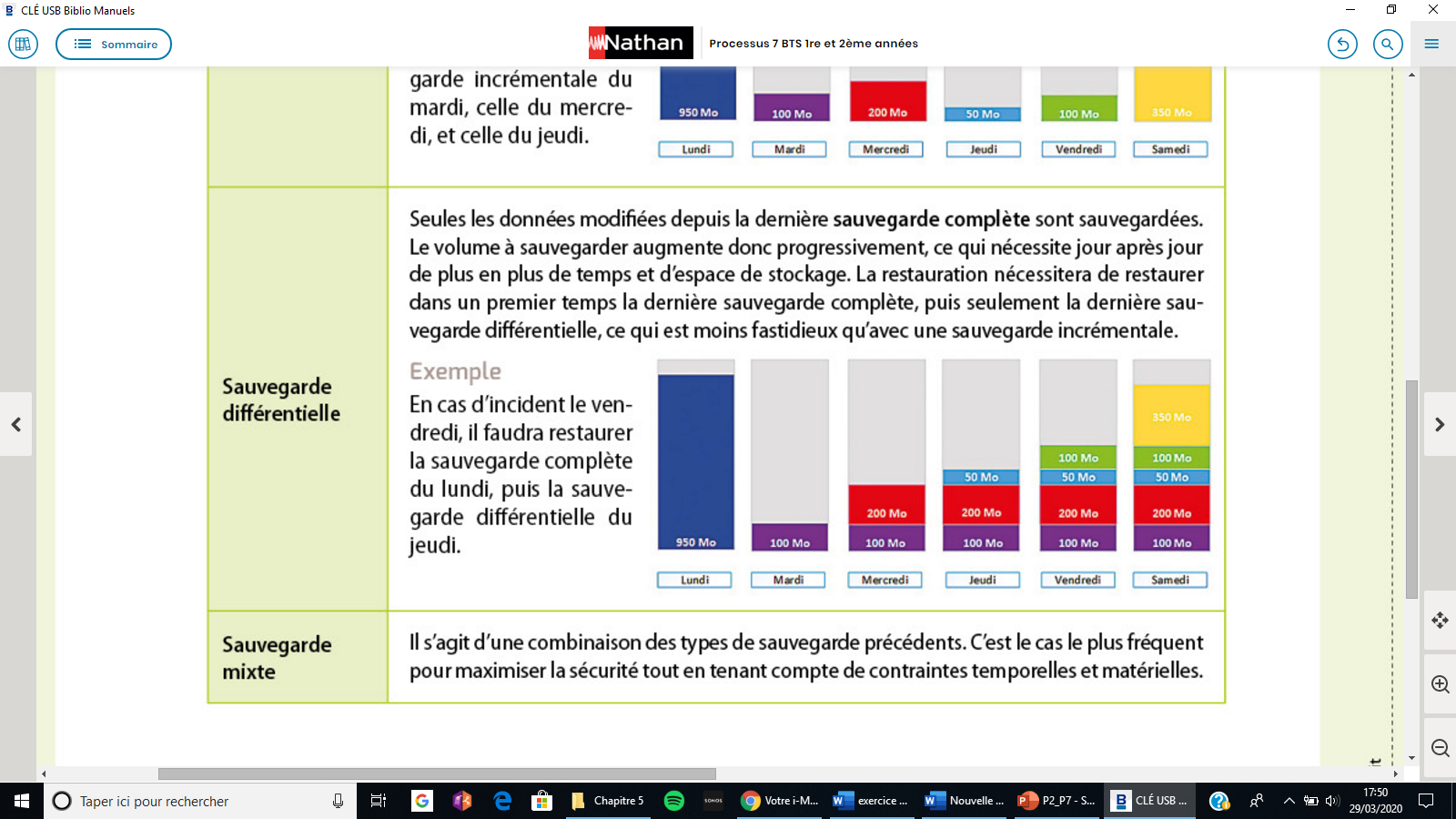
Il est installé à l’extérieur du bâtiment et connecté à la salle en amont de l’onduleur de manière à être déclencher dès que les batteries de l’onduleur sont vides.

**Un groupe électrogène** fonctionne au carburant : il faut donc gérer sa réserve et le réapprovisionner au besoin. Sa réserve doit pouvoir assurer une alimentation sur plusieurs jours.

# Protection des données

* L’installation d’un RAID est à instaurer permettant la répartition des données sur plusieurs disques améliorant les performances et la tolérance aux pannes.
* Effectuer des sauvegardes régulières

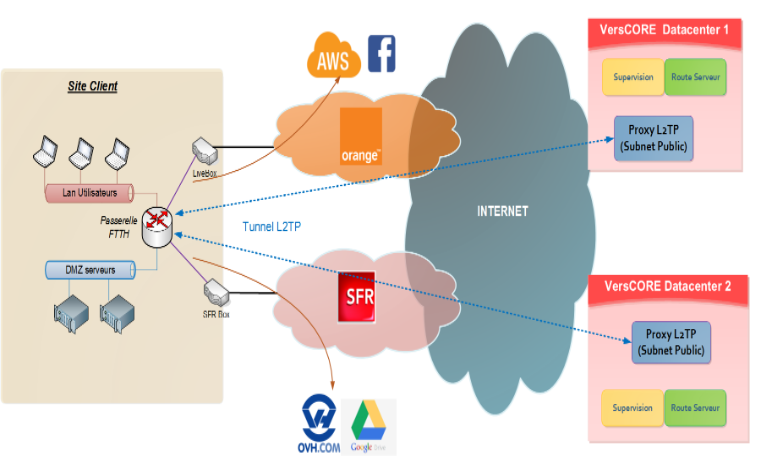




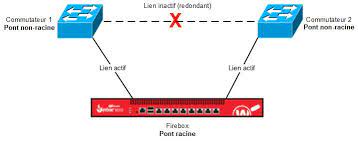
* Règles des 3,2,1 :
  + Au moins 3 sauvegardes des données
  + Sous 2 formats différents (cloud, disque, …)
  + 1 sauvegarde hors site
* Mettre le support de stockage des sauvegardes dans une armoire ignifugée dans une autre salle protégée et suffisamment éloigner pour qu’un incendie ne puisse pas l’endommager et hors sites



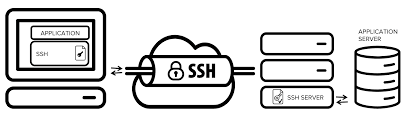
* Redondance de passerelle permettant un accès internet continu utile pour des sauvegardes dans le cloud (de l’entreprise ou d’un prestataire).



* **STP (Spanning-Tree Protocol) :** protocole de la couche 2 du modèle OSI évitant la formation de tempêtes de diffusion. Il permet de construire un arbre de chemin du moindre coût (à la meilleure bande passante) à partir d’un commutateur identifié comme pont racine.



* **Wake on lan :** permet de démarrer un poste à distance par le réseau
* **Tunnel SSH :** permettant de crée un accès à distance sécurisé au réseau.



* **Archivage « base active » :** la durée de conservation des données correspond à la durée de vie nécessaire pour accomplir la finalité de la donnée. (**ex :** les données relatives à un patient seront accessibles aux praticiens habilités le temps de sa prise en charge)
* **Archivage intermédiaire :** les données ont « rempli leur rôle initial » mais peuvent s’avérer nécessaires pour répondre à une obligation légale, ou constituer des éléments de preuves dans le cadre d’un contentieux
* Une analyse au cas par cas nécessaire pour dater la durée d’archivage
* Au niveau sécurité : lorsque les données passent de base active à l’archivage intermédiaire, ne doivent plus être consultables par tous les opérationnels initiaux, mais seulement par des personnes spécialement habilités (**ex :** le service en charge du contentieux)
* **Si les données sont archivées par un sous-traitant**, le responsable de traitement doit communiquer au sous-traitant la ou les durées dans le contrat de sous-traitance.