CESI

Projet SAS

GMSI 36

BOUTINAUD Romain
LAMONZIE Yvan

Table des matières

Présentation de la société EXTREME IT

Extreme IT est une société à responsabilité limitée au capital de 40 000€, fondé en 2006 par Mr et Mme DUPOND Eric et Roxanne, elle exerce l'activité de prestation informatique.

Situé 14 Rue des Mésanges à Mérignac (33700), à 15 minutes de Bordeaux centre et tous proche de la rocade extérieur, elle assure une proximité pour toute les entreprise de la région Bordelaise.

Elle est constituée de 11 employés dont 6 techniciens, 3 commerciaux, une assistante et le gérant.

Eric DUPOND
Gérant

Roxanne DUPOND
Assistante de direction

Archard DAVIGNON
Responsable Techniciens
Ingénieur système/Réseau

Romain BOUTINAUD
Technicien
Certification Microsoft MOS

Charlotte RICARD
Technicienne
Certification Microsoft MCITP

Yvan LAMONZIE
Technicien
Certification Cisco CCNA

Tristan LAFOND
Technicien
Certification C++ CPA

William COUDERT
Technicien
Certification SQL MCSA

Geoffrey CASGRAIN
Responsable Commercial

Rosemarie THIBAULT
Commercial

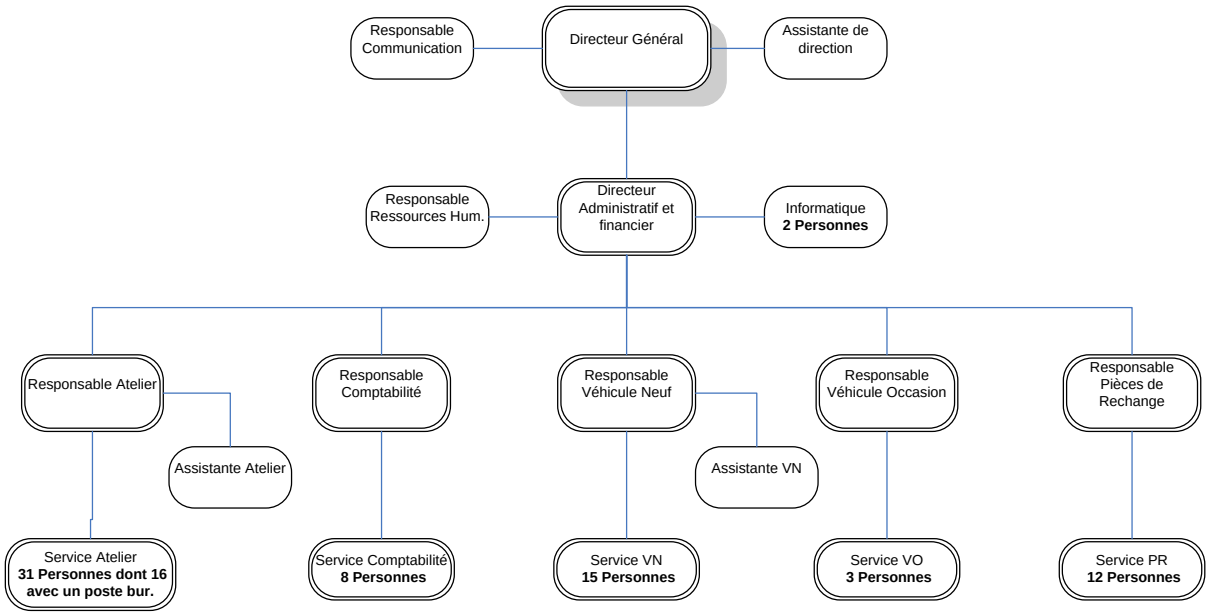
Théodore RIQUET
Commercial

RAPPEL DU CONTEXTE

L'entreprise du concessionnaire automobile « AutoConcept » (70 à 80 postes) souhaite externaliser les prestations informatiques aujourd'hui exécutées par deux informaticiens en internes.

Elle souhaite donc venir chez nous afin de garantir une continuité de service.

Organigramme de la société AutoConcept.



AutoConcept
70 avenue de la libération
Mérignac 33700
Tel : 0556452322
Siret : 1238RL284Z

AutoConcept nous a demandé de faire évoluer l'infrastructure informatique afin de pallier différents problèmes ayant trait à l'informatique.

Nous avons catalogué différents types de problèmes :

- Une perte d'argent suite à des pannes matérielles
- Des délais d'intervention trop longs
- Attitude désinvolte de la part des techniciens
- Pas de gestion des licences
- Aucune confidentialité des données

BOUTINAUD Romain
LAMONZIE Yvan

Synthèse légale de l'utilisation de l'informatique en entreprise

POINT SUR LA SITUATION ACTUELLE ET MISE A NIVEAU

L'entreprise a récemment été confrontée à plusieurs problèmes d'ordre légal au niveau de son système informatiques. Ces problématiques, que nous allons évoquer, sont largement évitables, et doivent absolument être évitées pour la bonne marche d'AutoConcept.

Avant toute mise en place d'un cadre légal, il est nécessaire de faire le point sur les comportements à risque et de trouver des solutions.

Dans un premier temps, pour empêcher toute nouvelle utilisation des postes de la société par des personnes non autorisées, nous préconisons la mise en place d'une politique de mots de passe par le biais de GPO, point sur lequel nous reviendrons dans la partie consacrée à la sécurisation des données.

Pour ce qui est de l'utilisation de logiciels Windows qui affichent une information « version de Windows pirates », il convient d'adopter une démarche stricte. En France, la contrefaçon de logiciels est punie de 3 ans d'emprisonnement et de 300.000 euros d'amende (Article L335-2 du Code de Propriété Individuelle), cette peine peut être amenée à 5 ans d'emprisonnement et 500.000 euros d'amende si la contrefaçon est considérée comme perpétrée en bande organisée.

La gestion des licences logicielles auprès d'une entreprise doit-être précise et sérieuse du fait de ces risques mettant en danger à la fois la personne morale mais aussi la personne physique qu'est son Directeur Général en tant que responsable légal (Article 121-2 du Code Pénal). Il est nécessaire d'œuvrer à cette mise en conformité le plus rapidement possible, certains consortiums offrent des rémunérations contre des informations sur l'utilisation de logiciels contrefaits, laissant la possibilité à des concurrents, anciens employés, clients mécontents de mettre en difficulté l'entreprise.

Les postes concernés étant arrivés en fin d'amortissement, nous proposons la résolution de cette problématique par le changement de ces ordinateurs.

La divulgation d'informations trouvées sur le poste d'un utilisateur est profondément inacceptable. C'est pour cette raison que l'informaticien mis en cause pour la précédente fuite de données ne sera pas conservé. L'accord conclu entre nos sociétés comprendra une clause de confidentialité (exemple en annexe), étendue à toute personne intervenant sur les matériels et/ou dans les locaux d'AutoConcept. Cette clause sera opposable devant les tribunaux.

Pour finir, le blocage de sites internet ou logiciels, doit faire l'objet, avant toute mise en place, d'une concertation avec les partenaires sociaux et d'une information à tous les salariés.

CADRE LEGAL

Il existe trois (3) limites principales au pouvoir de direction de l'entreprise en matière de contrôle et de surveillance des salariés, à savoir :

- La consultation des représentants des salariés et l'information des salariés. Article L 2323-32 du Code du Travail
- La proportionnalité des mesures de surveillance par rapport au but poursuivi. Article L1121-1 du Code du Travail
- La discussion entre l'employeur et les salariés ou ses représentants.

Les modalités de la surveillance informatique

Le Code du travail prévoit une information et une consultation des institutions représentatives du personnel " sur les moyens ou les techniques permettant un contrôle de l'activité des salariés " ainsi qu'un contrôle concernant, de manière plus générale, les " atteintes aux libertés individuelles ". Ces techniques de filtrage peuvent être mises en place dès lors qu'elles ont été portées à la connaissance des salariés et des représentants du personnel, dans les conditions prévues par le Code du travail.

La loi du 6 juillet 1978 (dite "informatique et libertés") impose, par ailleurs, que tout traitement automatique de données personnelles soit déclaré à la CNIL et le contrôle doit être " justifié par la nature des tâches " et " proportionné au but recherché ".

Filtrage de l'accès internet

Afin de garantir à la société une bande passante optimale ainsi qu'une productivité accrue, il est important que l'accès à internet soit limité. Nous proposons de nous servir d'un proxy (pfSense par exemple) qui peut se baser sur différentes listes.

Nous présentons des listes qui, à défaut d'être exhaustive, pourra servir de base de travail à la direction d'AutoConcept.

Autorisés :

- ✓ Sites à intérêt professionnel (Auto/Moto, assurances)
- ✓ Sites gouvernementaux
- ✓ Sites bancaires
- ✓ Sites scolaires

Interdits

- ✓ Sites à caractère érotique et/ou pornographique
- ✓ Sites de streaming
- ✓ Sites hébergeant des contenus illégaux
- ✓ Messageries instantanées

Autorisés à certains horaires (pause déjeuner)

- ✓ Réseaux sociaux

Déclarations à la CNIL

Vu les articles R10-12, R10-13 et R10-14 du Code des Postes et des Communications électroniques, la société doit conserver pour minimum trois (3) mois et maximum un (1) toutes les données de connexion de ses utilisateurs.

De ce fait, il est nécessaire de déclarer auprès de la CNIL différents fichiers. Nous en avons identifié au moins deux (2) :

- Fichiers de log des connexions aux sites internet externes.
- Fichiers de connexion et d'envoi de messages via la messagerie professionnelle.

Pour des raisons légales, le contenu des messages ne sera pas visible pour les techniciens intervenant chez AutoConcept. Il sera seulement à la disposition de l'autorité judicaire dans un cadre légal.

PLAN DE SECURISATION DES DONNEES

SAUVEGARDES

Afin de fiabiliser le système, nous proposons un système de sauvegardes multiples :

Dans un premier temps, nous allons mettre en place des clichés instantanés des serveurs. Cela améliore la protection et permet la disponibilité des documents en réalisant un stockage intelligent des données disponibles sur le réseau. En effet, il donne la possibilité aux utilisateurs de retrouver instantanément des versions précédentes de leurs fichiers sans devoir recourir à l'assistance d'une personne du service informatique.
Concrètement, on peut restaurer simplement des dossiers d'utilisateurs qui ont été supprimés par erreur ou mis à jour ; et les serveurs peuvent être configurés de façon transparente pour les utilisateurs ; permettant ainsi d'améliorer la productivité.

La deuxième opération est l'achat d'un second serveur pour soutenir le premier. Il sera configuré en réplication et placé dans une salle différente du premier serveur. Cela permet un accès aux données même en cas de problème physique sur le serveur actuel.

Pour compléter ces mesures, nous proposons la mise en œuvre d'une sauvegarde sur bande, qui permettra de sauvegarder les données de l'entreprise tous les soirs sur un support matériel et ainsi garder les cassettes dans un coffre-fort.

Pour pallier le défaut de la sauvegarde nocturne (perte possible de toutes les données du jour en cas de coupure avant le lancement), une sauvegarde instantanée sera effectuée sur un NAS situé dans la même salle que le deuxième serveur.

Le serveur actuel sera mis sous ondulation, pour éviter toute perte de donnée liée à une coupure de courant.

Le deuxième serveur sera le même que l'actuel avec quelques améliorations :

- Une deuxième alimentation en redondance.
- Une deuxième carte réseau en redondance.

Le serveur NAS sera de 6TO (la même taille que les disques durs des serveurs) en raid 1.

Le deuxième serveur ainsi que le NAS seront dans le bureau câblé et sécurisé, il manque cependant une climatisation et un onduleur pour assurer la continuité de l'activité en cas de panne électrique. Nous incluons ces équipements dans notre devis.

ACCES ET DISPONIBILITES DES DONNEES

Pour éviter tout accès non autorisé aux données de l'entreprise, nous proposons la mise en place d'un annuaire Active Directory. Cela permettra une gestion à la fois centralisée et personnalisée des différents droits des utilisateurs. Pour cela, il est nécessaire de faire la liste des utilisateurs ainsi que leurs droits quant aux différents dossiers.

Associé à cet annuaire d'utilisateurs, il convient de mettre en place une politique de mots de passe. Dans un premier temps, et surtout à titre indicatif, nous recommandons de suivre les conseils de la CNIL, à savoir : un mot de passe de 8 caractères minimums, composés de lettres chiffres et caractères spéciaux, dont la durée de validité n'excède pas trois (3) mois et avec une interdiction d'utiliser les trois (3) derniers mots de passe. Toutes ces limites pourront être spécifiées par GPO.

Couplé à cela, nous préconisons la mise à disposition de 48 Go d'espace sur les serveurs afin que les utilisateurs puissent y avoir accès même en cas de panne de leur poste personnel.

DIVERS

Du fait de l'intégration d'un des anciens techniciens à nos équipes, nous proposons sa mise à disposition en régie à la société AutoConcept. Il pourra ainsi agir plus vite en cas d'anomalies sur le réseau ou les postes. De plus, il connait déjà les employés et le fonctionnement d'AutoConcept.

Nous vous avons mis en devis des ordinateurs portables de dernière génération afin de remplacer les PC datant de plus de 3 ans.

Cela règlera les problèmes suivent :

- Toutes les licences Windows seront officielles,
- Les lenteurs ne se feront plus ressentir,
- Les postes pourront être déplacés très facilement,
- Les consommations électriques sont moins élevées par rapport à un ordinateur de bureau
- Les prix des ordinateurs portables sont moins élevés qu'un ordinateur fixe.

Les postes seront équipés de Microsoft Office starter.

BOUTINAUD Romain
LAMONZIE Yvan

CHARTE DE QUALITE SERVICE CLIENT

Compétences

EXTREME IT met son expérience et ses compétences au service du client. **EXTREME IT** se porte garant des compétences et de la disponibilité des personnes amenées à intervenir sous sa responsabilité comme des méthodes et outils utilisés.

Vous êtes assuré de la compétence et de la disponibilité de votre prestataire.

Confidentialité

EXTREME IT fournit à ses clients un système informatique respectant les dispositions législatives, règlementaires et déontologiques. **EXTREME IT** respecte et fait respecter par les personnes intervenant sous sa responsabilité le secret professionnel.

La confidentialité de vos données est assurée.

Contrôle qualité

EXTREME IT met en place un service spécialement chargé du lien entre le client et les équipes d'assistance.

Vous êtes assuré de la volonté d'amélioration permanente de la qualité du service d'information.

Ethique

Dans sa démarche commerciale,
EXTREME IT :

- ✓ Fournit des informations orales ou écrites précises, claires et sincères.
- ✓ Propose les solutions adaptées à l'activité et au budget du client.

Vous disposez d'un système d'information adapté à vos besoins

Evolutivité

EXTREME IT s'assure de la capacité à évoluer du système informatique du client.

Le système informatique du client s'adapte aux évolutions nécessaires.

Respect

Les techniciens **EXTREME IT** auront pour vous et vos relations professionnelles tous les égards dus à des clients.

Vous, vos clients et vos employés seront traités avec respect.

Responsabilité

Les responsabilités d'**EXTREME IT** sont formulées par contrat sur

- ✓ la nature des produits et services fournis
- ✓ l'étendue et les limites des garanties apportées à l'utilisateur.

Le client contracte avec un prestataire responsable.

Sécurité

EXTREME IT inclut dans le service d'informatisation la sûreté et la facilité d'exploitation du système informatique du client.

Vous disposez d'un système informatique sûr et d'utilisation aisée.

Services

EXTREME IT propose au client une gamme de services et un ensemble de prestations portant sur la mise en service, le suivi et la maintenance de son système informatique ainsi que sur la formation à son utilisation.

Le client peut compter sur un service de qualité.

BOUTINAUD Romain
LAMONZIE Yvan

MEMO INTERNE

Chers collaboratrices, collaborateurs,

Il importe, pour l'image de la société et sa bonne marche économique, que tous nos techniciens aient un comportement adapté lors de leurs contacts avec nos clients.

En tout lieu

Portez une tenue correcte.

Pensez aux formules de politesse et respectez vos clients.

Respectez les délais annoncés.

Soyez réactifs.

Répondez correctement au téléphone.

Soyez ponctuels. Si vous pensez être en retard, prévenez vos clients ET votre responsable.

Recueillez le consentement préalable de l'utilisateur avant toute prise en main à distance.

Les données de vos clients sont confidentielles, ne les partagez pas !

Chez le client

Respectez les employés et locaux de vos clients.

Vouvoyez vos clients.

Pensez à avoir à votre disposition du matériel de spare.

A l'agence

Utilisez l'outil de ticketing à bon escient :

- Traitez rapidement les demandes (H+4).
- Consignez toute intervention (téléphonique ou physique).
- Tenez à jour les inventaires de matériel.
- Demandez la fermeture du ticket lorsque l'incident est terminé.

Eric DUPOND
Gérant

Eric Dupond

CONCLUSION

Nous vous permettons avec ce dossier d'envisager une infrastructure informatique aux normes, avec une protection contre les coupures électriques, une multiplication des méthodes de sauvegarde afin d'éviter le plus possible la perte de donnée, et la continuité d'activité en cas de panne matérielle.

Nous vous garantissons aussi la rapidité des interventions avec la présence permanente d'un technicien dans les locaux d'AutoConcept. De plus, un suivi sera assuré via le site de ticketing et notre site de supervision.

Nous vous permettons aussi une évolution dans le futur afin de faire grandir l'infrastructure information en fonction de vos besoins.

ANNEXES

CLAUSE DE CONFIDENTIALITE

Je soussigné Monsieur/Madame ……., technicien de la société Extreme IT (ci-après dénommé «la Société»), étant à ce titre amené à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données. Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;

- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;

- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions;

- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;

- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité matérielle de ces données ;

- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;

- assurer, dans la limite de mes attributions, l'exercice des droits d'information, d'accès et de rectification de ces données ;

- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose notamment à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.

Fait à ……. le ../../…. en …. exemplaires

Nom :

Signature :

BOUTINAUD Romain
LAMONZIE Yvan

ENQUETE DE SATISFACTION AUTOCONCEPT

Votre Nom :

Adresse e-mail : ……@…… . …

Numéro d'intervention : AC……

Indiquez votre niveau de satisfaction relatif aux points suivants

Relation commerciale

	Très Satisfait	Satisfait	Insatisfait	Très Insatisfait	Non applicable
Qualité de l'accueil téléphonique	❑	❑	❑	❑	❑
Compréhension de la demande	❑	❑	❑	❑	❑
Qualité du conseil	❑	❑	❑	❑	❑
Réactivité commerciale	❑	❑	❑	❑	❑
Clarté des propositions et devis	❑	❑	❑	❑	❑

Performance de la solution

	Très Satisfait	Satisfait	Insatisfait	Très Insatisfait	Non applicable
Fiabilité du produit	❑	❑	❑	❑	❑
Ergonomie du produit	❑	❑	❑	❑	❑
Fonctionnalités du produit	❑	❑	❑	❑	❑

Activité technique et service après-vente

	Très Satisfait	Satisfait	Insatisfait	Très Insatisfait	Non applicable
Délais de livraison / installation	❑	❑	❑	❑	❑
Délais d'intervention / réparation	❑	❑	❑	❑	❑
Votre relation avec les techniciens	❑	❑	❑	❑	❑

Appréciation globale

	Très Satisfait	Satisfait	Insatisfait	Très Insatisfait
Votre appréciation globale	❑	❑	❑	❑

Recommanderiez-vous EXTREME IT à vos relations professionnelles ?

❑ Oui ❑ Non ❑ Peut-être

Commentaires

……
……
……
……
……

TEXTES DE LOI

Article L335-2 du Code de Propriété Intellectuelle

Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.
La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.
Seront punis des mêmes peines le débit, l'exportation et l'importation des ouvrages contrefaisants.
Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende.

Article 121-2 du Code Pénal

Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Article 34

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Article 35

Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.
Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.
Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.
Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

Article L1121-1 du Code du Travail

> Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

Article L2323-32 du Code du Travail

> Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.

Article R10-12 du Code des Postes et Communications électroniques

> Pour l'application des II et III de l'article L. 34-1, les données relatives au trafic s'entendent des informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi.

Article R10-13 du Code des Postes et Communications électroniques

> I. - En application du II de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :
>
> a) Les informations permettant d'identifier l'utilisateur ;
>
> b) Les données relatives aux équipements terminaux de communication utilisés ;
>
> c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
>
> d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
>
> e) Les données permettant d'identifier le ou les destinataires de la communication.
>
> II. - Pour les activités de téléphonie l'opérateur conserve les données mentionnées au I et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.
>
> III. - La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.
>
> IV. - Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

Article R10-13 du Code des Postes et Communications électroniques

> I. - En application du III de l'article L. 34-1 les opérateurs de communications électroniques sont autorisés à conserver pour les besoins de leurs opérations de facturation et de paiement les données à caractère technique permettant

d'identifier l'utilisateur ainsi que celles mentionnées aux b, c et d du I de l'article R. 10-13.

II. - Pour les activités de téléphonie, les opérateurs peuvent conserver, outre les données mentionnées au I, les données à caractère technique relatives à la localisation de la communication, à l'identification du ou des destinataires de la communication et les données permettant d'établir la facturation.

III. - Les données mentionnées aux I et II du présent article ne peuvent être conservées que si elles sont nécessaires à la facturation et au paiement des services rendus. Leur conservation devra se limiter au temps strictement nécessaire à cette finalité sans excéder un an.

IV. - Pour la sécurité des réseaux et des installations, les opérateurs peuvent conserver pour une durée n'excédant pas trois mois :

a) Les données permettant d'identifier l'origine de la communication ;

b) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

c) Les données à caractère technique permettant d'identifier le ou les destinataires de la communication ;

d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs.

BOUTINAUD Romain
LAMONZIE Yvan

DEVIS MATERIEL

Extreme IT
14 rue des Mésanges
33700 Mérignac
extreme.it33@gmail.com
Tel : 05 57 69 47 85

12 Novembre 2013

AutoConcept
70 avenue de la libération
Mérignac 33700
Tel : 05 56 45 23 22

DEVIS

numéro de devis : **842**

Désignation	Quantité	Prix unitaire HT	Total
Serveur + 1x onduleur + 1x bande de sauvegarde + 1x bande de nettoyage	1	6 676.00 €	6 676.00 €
Onduleur	1	300.00 €	300.00 €
Bande de sauvegarde	7	125.00 €	875.00 €
PC portable	52	549.12 €	28 554.24 €
Coffre fort	1	166.39 €	166.39 €
Climatisation	1	262.43 €	262.43 €
Serveur NAS	1	344.92 €	344.92 €
Logiciel de sauvegarde Acronis	2	650.00 €	1 300.00 €
Prestation heure installation	32	70.00 €	2 240.00 €
Exctincteur ABC 6kg	2	26.99 €	53.98 €
Total HT			**40 718.98 €**
T.V.A 19,6			**7 980.92 €**
Total TTC			**48 699.90 €**

Délai de réalisation : 3 semaines
Offre valable 3 mois

REFERENCES DEVIS MATERIEL

Dell Poweredge T320 + Lecteur de bandes

Référence catalogue :	**909 SVT320**
Base	PowerEdge T320, TPM
Option de Garantie Dell	3 ans de garantie de base - Intervention le jour ouvrable suivant incluse - Aucune extension de garantie sélectionnée
Carte réseau supplémentaire	On-Board Broadcom 5720 Dual Port 1GBE
Carte réseau supplémentaire	Broadcom 5720 DP 1Gb Network Interface Card
Gestion intégrée des systèmes	Basic Management
Configuration du châssis	3.5" Chassis with up to 8 Hot-Plug Hard Drives
Cadre	No Bezel
Paramètres BIOS de gestion de l'alimentation	Performance BIOS Setting
Configuration RAID	C16A - RAID 1/RAID 5 for H310/H710, 2 + 3-14 SAS/SATA/SSD HDDs, Max based on the Chassis
Contrôleur RAID	PERC H710 Adapter RAID Controller, 512MB NV Cache
Processeur	Intel® Xeon® E5-1410 2.80GHz, 10M Cache, Turbo, 4C, 80W, Max Mem 1333MHz
Capacité de mémoire	(2) 4GB UDIMM, 1600 MHz, Low Volt, Dual Rank, x8 Data Width
Type et vitesse de mémoire DIMM	1600 MHz UDIMMs
Type de configuration de la mémoire	Performance Optimized
Disques durs	(2) 500GB, SATA, 3.5-in, 7.2K RPM Hard Drive (Hot Plug)
Disques durs (2e groupe)	(4) 1TB, SATA, 3.5-in, 7.2K RPM Hard Drive (Hot Plug)
Stockage amovible	LTO-6 Internal Tape Drive with Controller
Support de stockage	LTO Tape Cleaning Cartridge
Lecteur optique interne	DVD ROM, SATA, Internal
Rails pour rack	Tower Chassis, No Casters
Alimentation	Dual, Hot-plug, Redundant Power Supply (1+1), 495W
Cordons d'alimentation	(2) European Power Cord 220V
Système d'exploitation installé en usine	Windows Server 2008 R2 SP1, Standard Edition, French, Incl. 5 CALs, No Media
Kits de supports SE	DVD Media for Windows Server 2008 R2 SP1, Standard Edition, French

Onduleur Dell UPS Tower 1000W

Référence catalogue :	**909 UPS1000WTU**
Module	Description
Base	Dell UPS, Tower, 1000W, 230V, incl. Cable Pack
Bundle	UPS1000WTU
Garantie de base	Tower 500/1000/1920/2700W 3Yr Parts Only Warranty
Options de Garantie Dell	3Yr Parts Only Warranty Included - No Upgrade Selected

Ordinateur portable

Référence catalogue :	**909 CN37102**
Processeur	Inspiron 17
Système d'exploitation	Windows 7 64bit , Français
Mémoire	1 module DIMM DDR3L de 4 Go (1 x 4 Go) à 1 600 MHz
Clavier	Clavier intégré, français (AZERTY)
Carte graphique	Carte graphique HD Intel®
Pilote	Pilote Dell™ Wireless 1704/1705
Disque dur	Disque dur Serial ATA de 500GB (5 400tr/min)
Lecteur optique	Lecteur DVD+/-RW 8X
Connectivité sans fil	Carte Dell™ Wireless 1705 802.11b/g/n avec Bluetooth v4.0
Options de Garantie Dell	3 ans de service à domicile le jour suivant avec support téléphonique Premium
Batterie principale	Batterie principale à 4 cellules (40 W/h) au lithium-ion
Processeur	Processeur Intel® Pentium® 2127U (2M Cache, 1.9GHz)
Couleur du capot	Panneau arrière de l'écran LCD : noir
FGA Module	OAK17V_1405_227/FR/BTS
Logiciel optique	CyberLink
Value Added Services	Assistance téléphonique Premium incluse dans votre garantie étendue
Informations de vente au détail	Inscription Vente au détail 2.0
Ecran LCD	Écran rétroéclairé 17,3" avec technologie TrueLife et résolution HD+ (1 600 x 900)

Serveur NAS :

	Livré avec 2 disques durs
Dimensions	146,4 x 115 x 178,5 mm
Poids	0,6 kg
Processeur	Marvell Kirkwood 88F6702 à 1,0 GHz
Mémoire vive	256 Mo
Alimentation interne (intégrée)	Non
Refroidissement passif sans ventilateur	Non
DISQUE	
Capacité (totale)	6 To
Baies	boitier 2 baies
Format de baie	Pour disque 3,5"
Interface disque	SATA
Géométrie disques (RAID)	JBOD, Raid 0, 1
INTERFACE ET CONNECTIQUE	
Connexion réseau	Gigabit Ethernet
Plusieurs ports réseau	Non
Port(s) eSATA	Non
Ports(s) USB	1 port USB 2.0
Cible iSCSI	Non
Garantie	2 ans

Climatisation

Marque	**WHIRLPOOL**
Type de produit	Climatiseur mobile
Modèle	AMD081/1
Type de chauffe	Rayonnant
Puissance frigorifique	2800 W
Plus produit	Fonction " 6ème sens" Fonction "round U"
Fixation	Roulettes
Dimensions	Profondeur : 36 cm Largeur : 46 cm Hauteur : 84 cm
Couleurs	Blanc
Poids	35 Kg
Programmation	Minuterie 24 H
Soufflerie	Préconisée pour une surface de 28 à 37m²
Affichage	Ecran LCD Indicateur de saturation du filtre, du réservoir Indicateur température télécommande
Fonctions du produit	Fonction Jet/Turbo Mode nuit Oscillation automatique 3 Vitesses + Auto Déshumidification 1 L / H

Type de gaz	R410a
Type de filtre	Pré-filtre anti-poussières lavable
Pression sonore	65 dBa
Raccord	cable 1.5 m Diamètre de la gaine : 16 cm
Alimentation	220 -240V 50 Hz 20 A Consommation 1.1 KW
Eléments livrés	Télécommande
Classe énergétique	A
Garantie	1 an pièce

Coffre-fort ignifugé Titan II PHOENIX - FS1271E

Protection contre le feu pour le papier et données numériques :
Papier : Testé par la norme standard Internationale NT Fire 017 – 60, au centre Suédois SP Testing Centre ; le coffre protège les documents papier pendant 60 minutes.
Données numériques : Testé par la norme standard au feu MTC-DIP 120-60DM, le coffre protège les données numériques; DVD, Clefs USB, Cartes mémoires, pendant 60 minutes.

Verrouillage par serrure numérique hauté sécurité. Ecran LCD programmable par code utilisateur à 6 chiffres. En cas d'erreur, un système d'alarme intégré se met en marche pour alerter d'une tentative d'intrusion

Résistance au feu :

Ce modèle peut résister contre le feu durant 60 minutes à une température de 945°C, selon la norme International Standard NT FIRE 017 60. La protection est totale, et la dégradation de vos documents papier et numériques est quasi nulle grâce à cet appareil.

Caractéristiques techniques

Dimensions externes (H*L*P en mm) : 308*410*342
Dimensions internes (H*L*P en mm) : 220*330*225
Ouverture de la porte/ Profondeur de la poignée de porte : 380mm/40mm
Poids : 26 kg
Capacité : 16L
Crochets et clés à l'intérieur : 4

Garantie 2 ans

Extincteur

- Homologué conforme à la norme CE **97/23/CE** quant aux risques de pression.

- Répond aux exigences européennes **EN 3-7+A1.**

- Certifié **AENOR**

- Corps en acier.

- Robinet d'arrêt en laiton.

- Système de dispersion amélioré et simple d'utilisation.

- Surface extérieure obtenue par poudrage électrostatique et cuisson au four.

- Surface interne des appareils à base d'eau par plastification.

- Ouverture de l'appareil simplifiée (sans outil) mais doit être toujours effectuée par une personne compétente.

- Valve de pressurisation normalisée.

- Poids : 9.22 Kg**.**

Garantie 1 an

BOUTINAUD Romain
LAMONZIE Yvan

DEVIS DE PRESTATION

Extreme IT
14 rue des Mésanges
33700 Mérignac
extreme.it33@gmail.com
Tel : 05 57 69 47 85

12 novembre 2013

AutoConcept
70 avenue de la libération
Mérignac 33700
Tel : 05 56 45 23 22

DEVIS

numéro de devis : **843**

Désignation	Quantité	Prix unitaire HT	Total
Prestation horaire mensuelle	151	27.00 €	4 077.00 €
Total HT			**4 077.00 €**
T.V.A 19,6			**799.09 €**
Total TTC			**4 876.09 €**

Offre valable 3 mois
Contrat d'un an

GLOSSAIRE

Active Directory : C'est l'un des services compris dans la licence de Windows serveur, Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone, etc.) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données, etc.

Bande de sauvegarde : C'est le même principe et la même apparence qu'une cassette vidéo mais pour enregistrer des données.

Déploiement par GPO : (Group Policy Object) Procédure qui permet le déploiement d'application ou de stratégie au démarrage de l'ordinateur. Cela permet une gestion unifiée du système informatique.

Disque dur : C'est le support de stockage des données.

Ethernet : type de câble pour l'interconnexion dans appareil réseaux.

Go : (Giga Octets) Unité de mesure informatique (1 Go = 1024 Mo).

LTO 6 : (Linear Tape-Open) technique de stockage sur bande de sauvegarde.

NAS : (Network Attached Storage) C'est un petit ordinateur conçu pour le stockage.

Onduleur : En cas de coupure électrique, l'onduleur est capable de fournir de l'électricité pendant un certain temps grâce à ces batteries.

Raid 1 : (Redundant Array of Independent Disks) C'est la configuration de plusieurs disques durs en miroir (toutes les données sont copiées sur le premier et sur le deuxième disque dur). En cas de panne sur un disque dur, le deuxième prend le relai sans perdre aucune donnée.

Raid 5 : (Redundant Array of Independent Disks C'est un compromis entre la sécurité et la performance, il faut 3 disques durs au minimum.

RAM : (Random Access Memory) C'est la mémoire vive, c'est un support de stockage très rapide qui s'efface dès que l'ordinateur s'éteint.

RJ45 : Type d'embout pour le câble Ethernet

Serveur : C'est un gros ordinateur très puissant

To : (Téra Octets) Unité de mesure informatique (1 To = 1024 Go)

CHARTE INFORMATIQUE

Préambule

L'entreprise AutoConcept met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique.

Les salariés, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens de communication mis à leur disposition et à les utiliser.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources.

1. Champ d'application

Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut, y compris les mandataires sociaux, salariés, intérimaires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels.

Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

Système d'information et de communication

Le système d'information et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, logiciels, fichiers, données et bases de données, système de messagerie, intranet, extranet.

2. Confidentialité des paramètres d'accès

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants, mots de passe).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs.

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par le Service Informatique afin de recommander les bonnes pratiques en la matière.

3. Protection des ressources sous la responsabilité de l'utilisateur

L'entreprise met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

Le Service Informatique est responsable du contrôle du bon fonctionnement du système d'information et de communication. Il veille à l'application des règles de la présente. Les membres du Service Informatique sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître.

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

L'utilisateur doit éviter d'installer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'entreprise. Il doit dans tous les cas en alerter le Service Informatique.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

4. Accès à Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le Service Informatique. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers. Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur Internet.

5. Messagerie électronique

La messagerie électronique est un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par le Service Informatique.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer le Service Informatique des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'entreprise et/ou de l'utilisateur.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

En cas d'envoi à une liste de diffusion, il est important de vérifier la liste des abonnés à celle-ci, l'existence d'archives accessibles par le public et les modalités d'abonnement.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

Limites techniques

La taille, le nombre et le type des pièces jointes peuvent être limités par le Service Informatique pour éviter l'engorgement du système de messagerie.

Les messages électroniques sont conservés pendant une durée de 365 jours maximum. Passé ce délai, ils sont automatiquement supprimés. Si le salarié souhaite conserver des messages au-delà de ce délai, il lui appartient d'en prendre copie.

Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les messages envoyés doivent être signalés par la mention " Privé " dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé " Privé ". Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé " Privé ". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Utilisation de la messagerie pour la communication destinée aux institutions représentatives du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel.

6. Données personnelles

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés. Elle institue au profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers. Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la présente charte. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978.

7. Contrôle des activités

Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (" logs "), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information. Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications suppression de fichiers
- aux connexions entrantes et sortantes au réseau interne,
- à la messagerie
- et à Internet,

pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers .L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le Service Informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Lorsque le contrôle porte sur les fichiers d'un utilisateur et sauf risque ou événement particulier, le Service Informatique ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier.

Le contenu des messages à caractère personnel des utilisateurs (tels que définis à l'article 4 des présentes), ne peut en aucun cas être contrôlé par le Service Informatique.

8. Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées la gravité des faits concernés.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

9. Information des salariés

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié.

Le Service Informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des NTIC. Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

10. Entrée en vigueur

La présente charte est applicable à compter du

SOURCES

- www.qualiblog.fr
- www.olfeo.com
- www.dell.fr
- www.materiel.net
- www.cdiscount.fr
- www.wikipedia.fr
- www.coffrefortplus.fr
- www.ylea.eu
- www.legifrance.gouv.fr
- www.cnil.fr