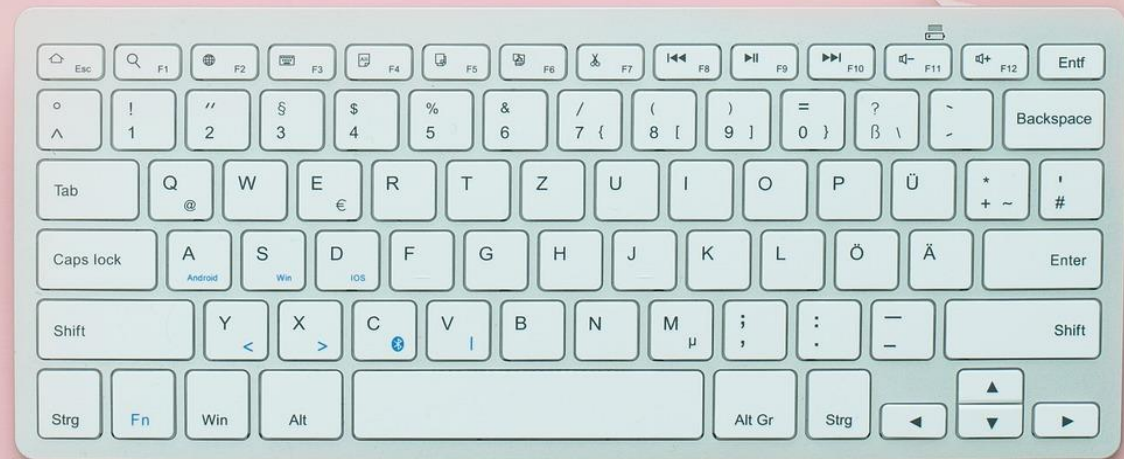


INTRODUCTION AU DROIT INFORMATIQUE



DROIT DU NUMÉRIQUE

- L'utilisation des systèmes d'information
- Les flux de données professionnelles et personnelles
- Les logiciels de traitement
- Les droits des personnes

DROIT DES CONTRATS

- La relation utilisateur sur internet
- Les Conditions Générales
- La responsabilité sur internet

DROIT DE LA CONSOMMATION

- La vente sur internet
- La vente à distance
- Les droits des consommateurs
- La responsabilité des professionnels

LE DROIT DU NUMERIQUE



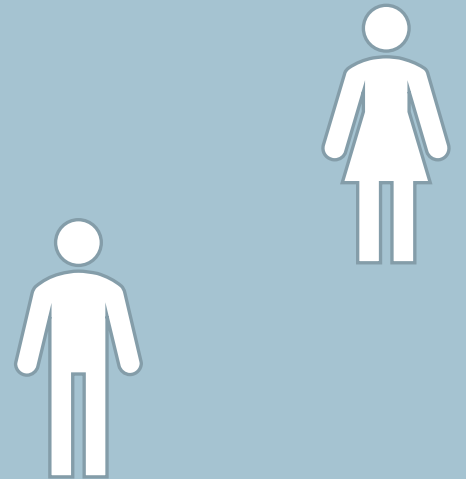
L'UTILISATEUR CONSOMMATEUR

**Particulier, personne physique,
il est celui que l'on protège sur
internet**

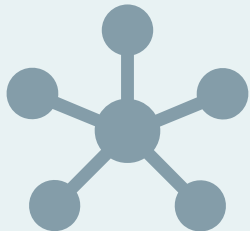


L'UTILISATEUR PROFESSIONNEL

**Il est celui qui édite sur un
site internet ou se présente à
l'utilisateur comme un
professionnel**



L'UTILISATION DES SYSTÈMES D'INFORMATION

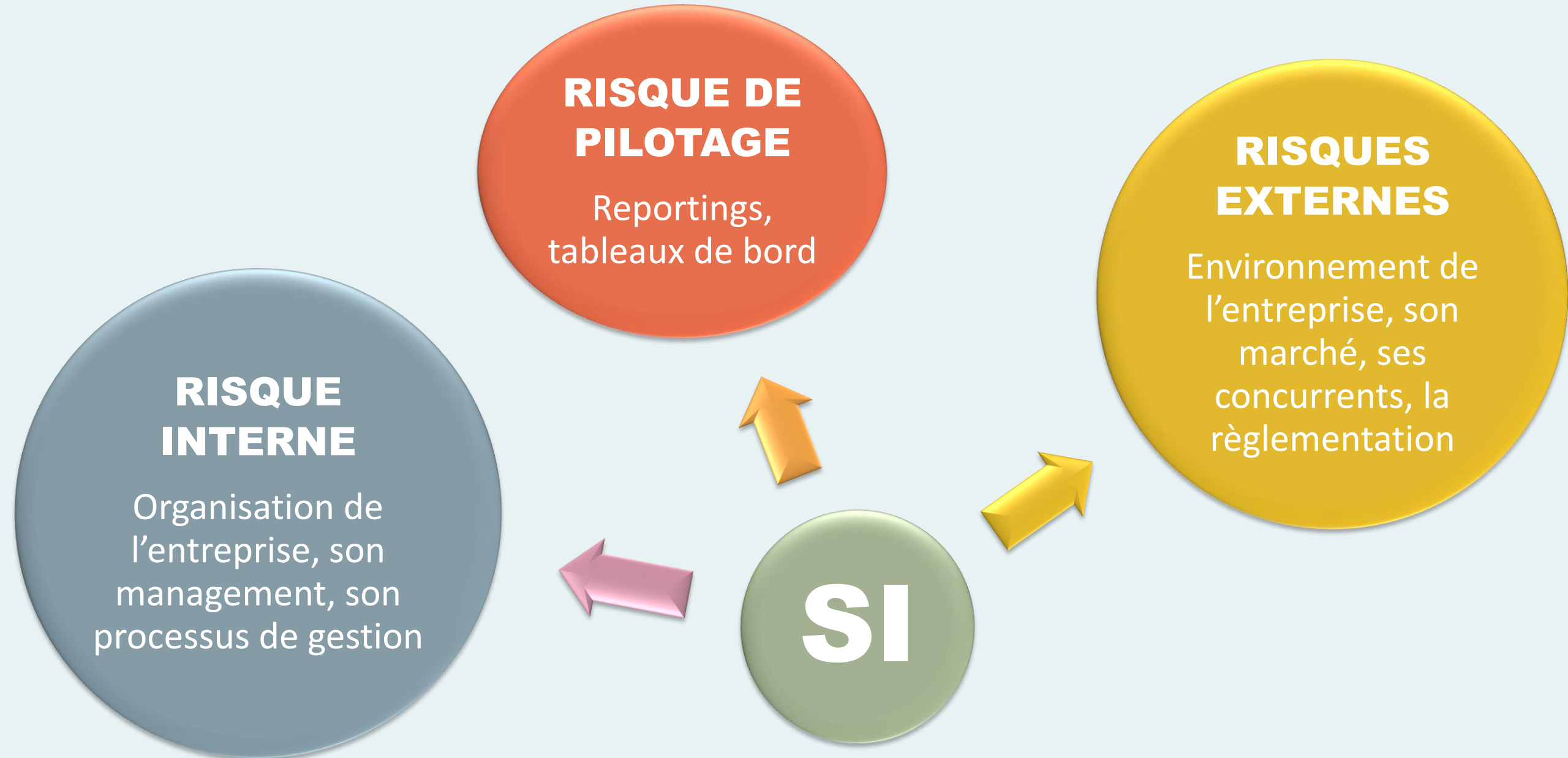


Le système d'information dans l'entreprise peut-être défini comme l'ensemble des acteurs (personnel, matériel, données) collectant, traitant, mémorisant et diffusant des données, à caractère professionnel et personnel.

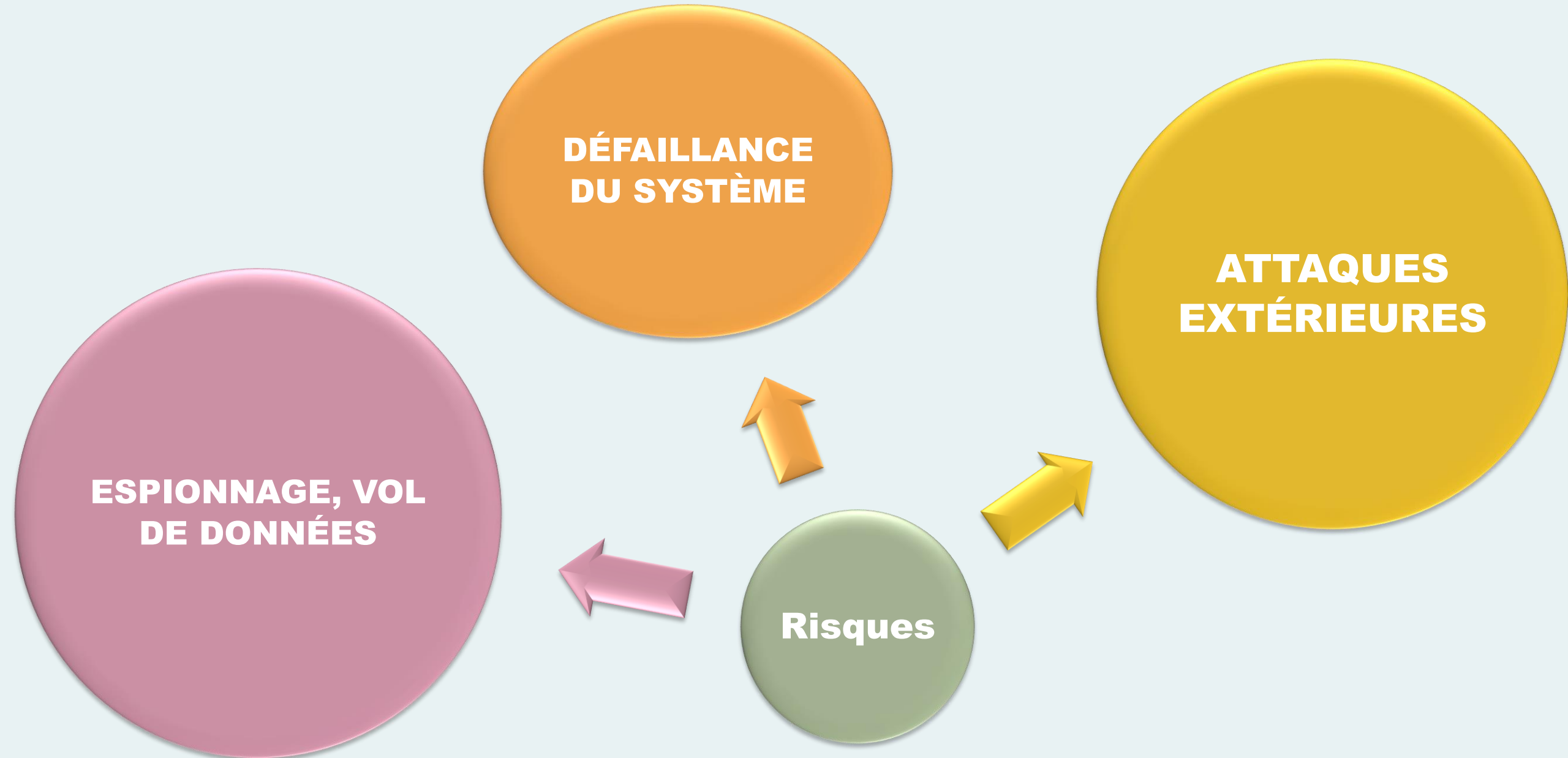
Il permet de transmettre et collecter les informations opérationnelles nécessaires au bon fonctionnement de l'entreprise.

Il s'analyse principalement par les différents flux de données repérés dans l'entreprise, en interne et en externe.

RISQUES LIES AUX SI INFORMATISES



RISQUES LIES AUX SI INFORMATISES



RISQUES LIES AUX SI INFORMATISES



The diagram consists of six 3D hexagonal blocks arranged in two rows of three. Each block is a different color and contains a risk category in white text. The top row contains 'Technique' (yellow), 'Organisationnel' (orange), and 'Humain' (purple). The bottom row contains 'Image de marque' (orange), 'Financier' (pink), and 'Juridique' (blue). The blocks have a slight 3D effect with shadows.

Technique

Organisationnel

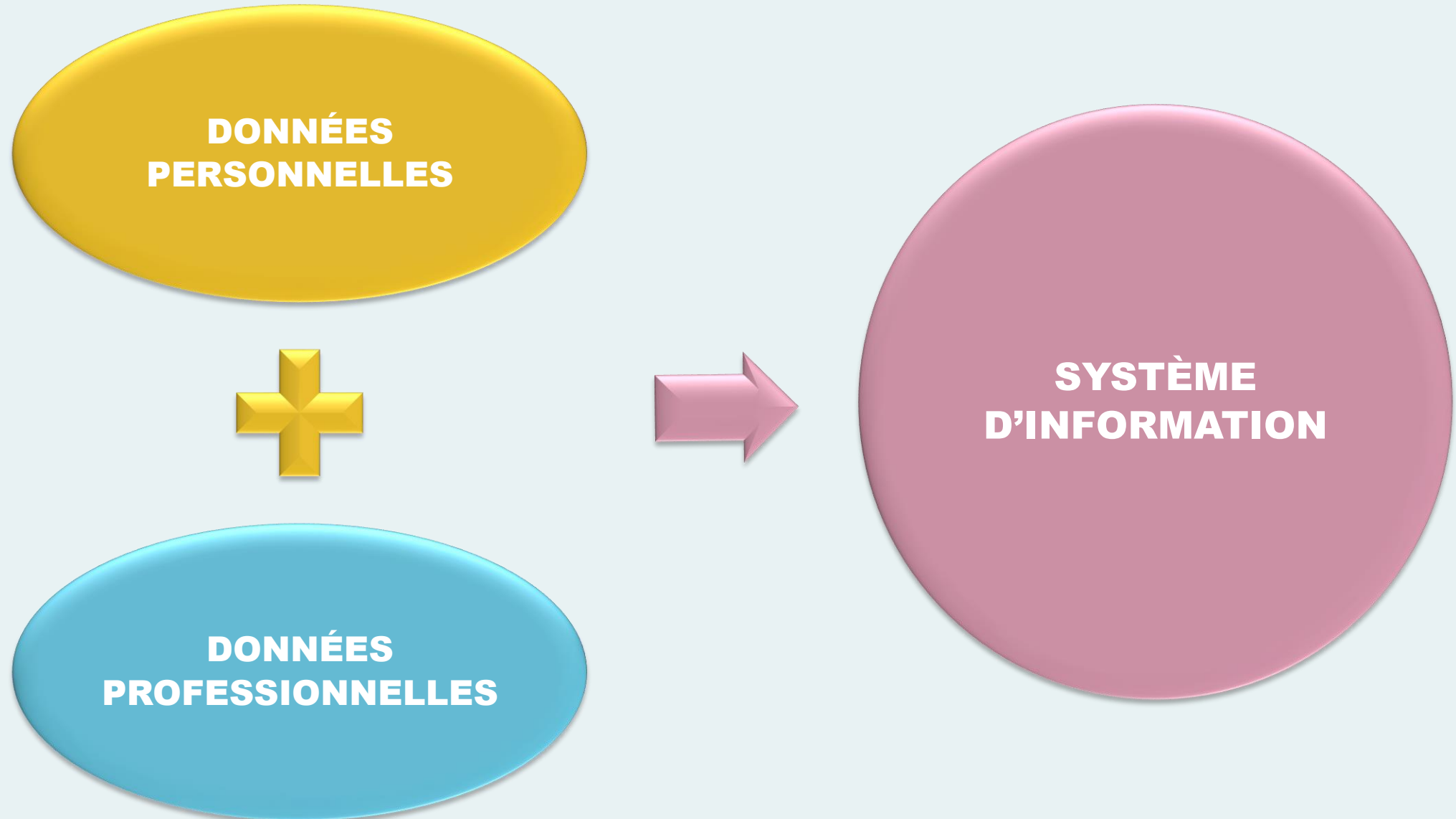
Humain

**Image de
marque**

Financier

Juridique

DONNEES DU SI



LES DONNEES PERSONNELLES DANS LE SYSTÈME D'INFORMATION



LES DONNEES PERSONNELLES DANS LE SI

De nombreuses données personnelles sont en circulation dans le SI des entreprises :

- **Coordonnées des salariés**
- **Coordonnées des clients**
- **Coordonnées des responsables des entreprises partenaires**
- **Les échantillons vocaux**
- **Les écoutes**
- **La surveillance**
- **La vidéo**
- **La GPS**
- **Les données médicales**



QU'EST CE QU'UNE DONNÉE PERSONNELLE ?



«DONNÉES À CARACTÈRE PERSONNEL»

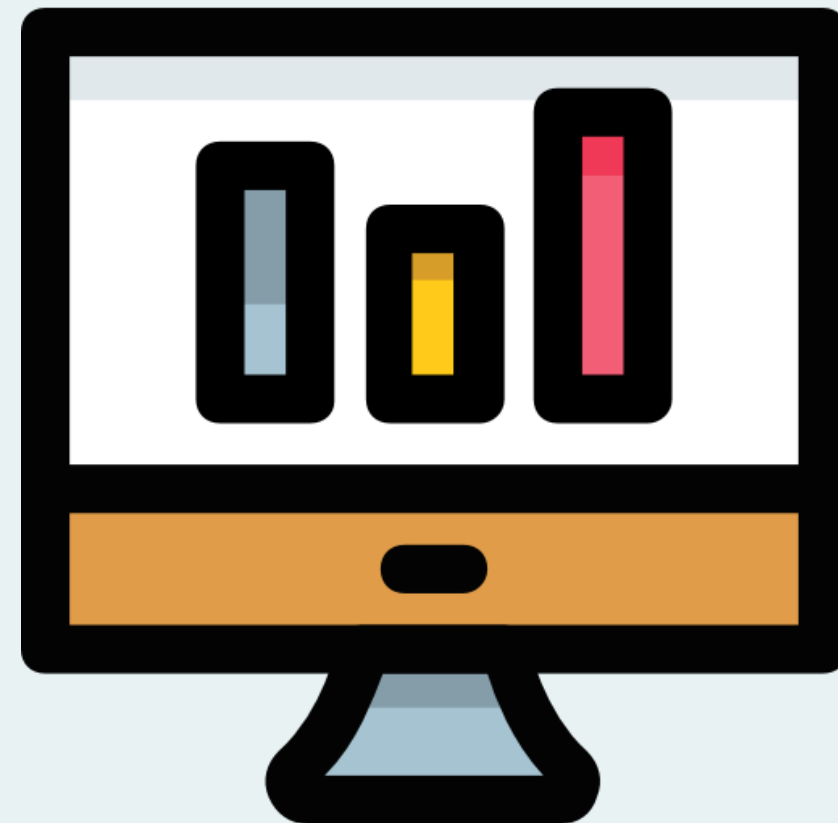
Toute information se rapportant à une **personne physique identifiée ou identifiable** telle que :

- nom
- **numéro d'identification**
- des données de localisation
- **un identifiant en ligne**
- un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

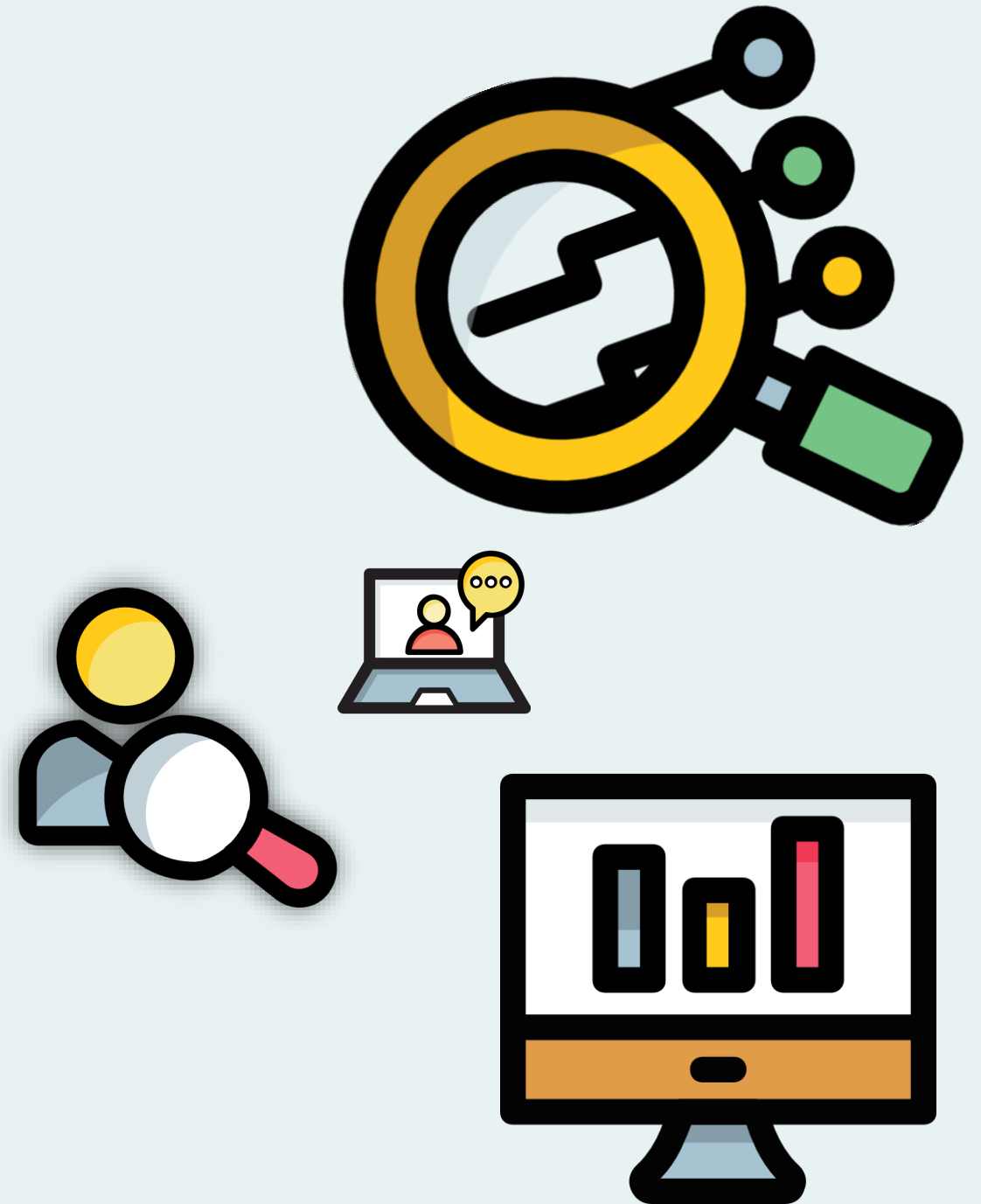
LE TRAITEMENT DE LA DONNEE PERSONNELLE

«TRAITEMENT»

- La Collecte
- L'enregistrement
 - L'organisation
- La Conservation
- La Modification
 - L'extraction
- La Consultation
 - L'utilisation
- La Communication Par Transmission
 - La Diffusion
- Le Rapprochement Ou L'interconnexion
 - L'effacement Ou La Destruction



**La collecte des
données
personnelles est
encadrée par le
RGPD, Règlement
Européen de
Protection des
Données entré en
vigueur le 25 mai
2018.**

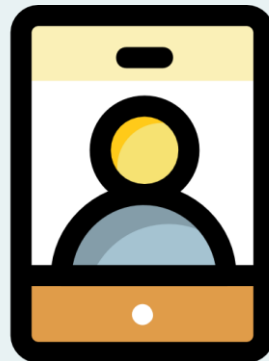


Champ d'application du RGPD

S'applique au traitement de données à caractère personnel, contenues ou appelées à figurer dans un fichier.

Il s'applique au traitement lorsque :

- **Le responsable est établi sur le territoire de l'union européenne.**
- **Le traitement est effectué en Union européenne**
- **Un résident européen est ciblé**



CONDITIONS DE LICÉITÉ DE COLLECTE DES DONNÉES

1. PRINCIPE DE **FINALITÉ** – ART 5

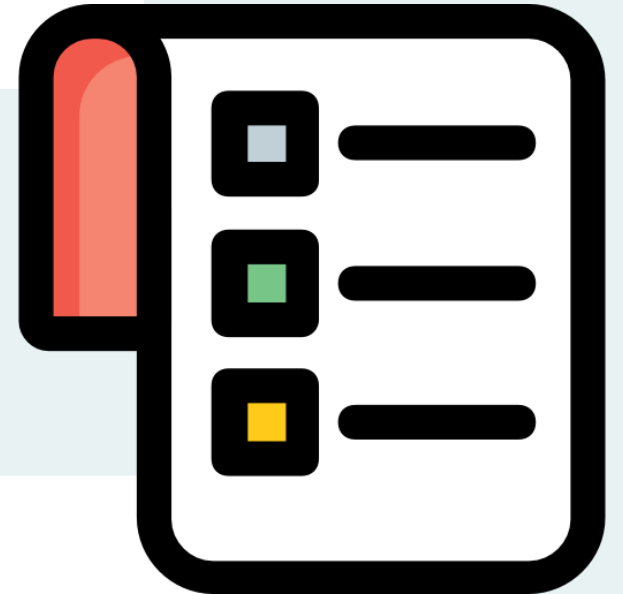
Les données personnelles recueillies et traitées doivent servir à l'usage légitime et déterminé défini dès le début par le responsable de la collecte.

2. PRINCIPE DE **PROPORTIONNALITÉ** – ART 5

L'importance et la quantité de données recueillies doivent être absolument nécessaire au but recherché par le responsable.

3. PRINCIPE DE **PERTINENCE** – ART 5

Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs



CONDITIONS DE LICÉITÉ DE COLLECTE DES DONNÉES

4. PRINCIPE DE **DURÉE** – ART 5

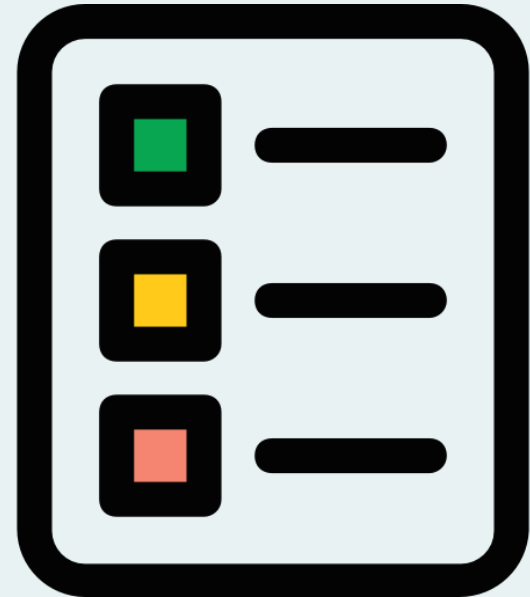
Les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

5. PRINCIPE DE **SÉCURITÉ** – ART 5

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.

6. PRINCIPE DE **TRANSPARENCE** – ART 5

Toutes les personnes dont les données personnelles ont été collectées ont un droit d'accès et de regard à ces informations.



CONDITIONS DE LICÉITÉ DE TRAITEMENT DES DONNÉES



- ✓ **La personne concernée a consenti** au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques
- ✓ **Le traitement est nécessaire à l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci
- ✓ **Le traitement est nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis

CONDITIONS DE LICÉITÉ DE TRAITEMENT DES DONNÉES

- ✓ **Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique**
- ✓ **Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement**
- ✓ **Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement**



AXE DE PRIORITÉ RGPD : LE CONSENTEMENT

- ✓ **Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant :**
 - au moyen d'une **déclaration écrite**, y compris par voie électronique
 - d'une **déclaration orale**
 - en **cochant une case** lors de la consultation d'un site internet
 - en **optant pour certains paramètres techniques** pour des services de la société de l'information
 - au **moyen d'une autre déclaration ou d'un autre comportement** indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel

**IL NE SAURAIT DÈS LORS Y
AVOIR DE CONSENTEMENT
EN CAS DE SILENCE,
DE CASES COCHÉES PAR
DÉFAUT OU D'INACTIVITÉ.**





DROITS DES PERSONNES



DROIT DE NE PAS DONNER SON CONSENTEMENT



Toute personne physique a **le droit de s'opposer**, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.

DROIT D'ÊTRE INFORMÉ AVANT LE TRAITEMENT

- **L'identité et les coordonnées du responsable du traitement**
- **Les coordonnées du délégué à la protection des données;**
- **Les finalités** du traitement
- **Les intérêts légitimes** poursuivis
- **Les destinataires** des données
- **Le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale**



DROIT D'ÊTRE INFORMÉ AVANT LE TRAITEMENT

- **La durée de conservation** des données
- **L'existence du droit de demander au responsable du traitement :**
 - **L'accès aux données à caractère personnel**
 - **La rectification**
 - **L'effacement de celles-ci**
 - **La limitation du traitement relatif à la personne concernée**
 - **Du droit de s'opposer au traitement et du droit à la portabilité des données;**
 - **Le droit d'introduire une réclamation auprès d'une autorité de contrôle**



DROIT DE LIMITER LE TRAITEMENT



La limitation du traitement correspond au marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur.

Il s'agit en fait de geler l'utilisation de vos données personnelles le temps de la vérification du motif de collecte. Le responsable doit alors cesser d'utiliser la donnée mais il doit la conserver.

DROIT DE LIMITER LE TRAITEMENT

LA LIMITATION DU TRAITEMENT PEUT ÊTRE DEMANDÉE LORSQUE :

- L'exactitude des données à caractère personnel est contestée
- Le traitement est illicite
- Le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice;
- La personne concernée s'est opposée au traitement



DROIT A L'OUBLI

La personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant lorsqu'un motif légitime s'applique.



DROIT A L'OUBLI

- a) Les données à caractère personnel ne sont plus nécessaires au regard des finalités**
- b) La personne concernée retire le consentement, et il n'existe pas d'autre fondement juridique au traitement;**
- c) La personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement**
- d) Les données à caractère personnel ont fait l'objet d'un traitement illicite**
- e) Les données à caractère personnel doivent être effacées pour respecter une obligation légale**
- f) Les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information**



DROIT A L'OUBLI

CE DROIT NE S'APPLIQUE PAS :

- ✓ À l'exercice du droit à la liberté d'expression et d'information
- ✓ Pour respecter une obligation légale ou pour exécuter une mission d'intérêt public
- ✓ Pour des motifs d'intérêt public (domaine de la santé publique)
 - ✓ À des fins archivistiques dans l'intérêt public
 - ✓ À des fins de recherche scientifique ou historique
 - ✓ À des fins statistiques
- ✓ À la constatation, à l'exercice ou à la défense de droits en justice.



DROIT A LA PORTABILITE



Les personnes dont les données font l'objet d'un traitement ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement,

DROIT D'OPPOSITION ET PRISE DE DÉCISION INDIVIDUELLE AUTOMATISÉE

«PROFILAGE»

Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant :

- le rendement au travail
- la situation économique
 - la santé
- les préférences personnelles
 - les intérêts
 - la fiabilité
- le comportement
- la localisation ou les déplacements de cette personne physique



DROIT D'OPPOSITION ET PRISE DE DÉCISION INDIVIDUELLE AUTOMATISÉE

**La personne concernée a le droit de ne pas faire l'objet d'une
décision fondée exclusivement sur un traitement automatisé, y
compris le profilage, produisant des effets juridiques la
concernant ou l'affectant de manière significative de façon
similaire.**





LES DROITS DES SALARIES SUR LEURS DONNEES AU TRAVAIL

LES FICHIERS ET DONNÉES PERSONNELS DU SALARIÉ SUR SON ORDINATEUR PROFESSIONNEL

- **Tous les fichiers présents sur l'ordinateur professionnel sont réputés être professionnels SAUF s'ils sont strictement identifiés comme étant PERSONNELS.**
- **Il en est de même pour les fichiers stockés sur une clé USB reliée à l'ordinateur professionnel et sur des discs durs externes appartenant à l'entreprise et des Clouds.**



LES FICHIERS ET DONNÉES PERSONNELS DU SALARIÉ SUR SON ORDINATEUR PROFESSIONNEL

Attention toutefois à prendre quelques précautions :

- **Indiquer seulement ses noms et prénoms ne rend pas le dossier personnel**
- **Un salarié ne peut pas nommer son ordinateur entier « personnel »**
- **Insérer le caractère personnel en objet des mails personnels**
- **Supprimer fréquemment l'historique de ses navigations et rester en privé**



LES FICHIERS ET DONNÉES PERSONNELS DU SALARIÉ SUR SON ORDINATEUR PROFESSIONNEL

SONT INTERDITS POUR L'EMPLOYEUR

- La mise en place de keyloggers
- La télémaintenance et la prise de contrôle à distance à l'insu du salarié
- L'interdiction totale du stockage de fichiers personnels sur l'ordinateur professionnel

IL POURRA TOUTEFOIS

- Restreindre ou interdire la navigation sur des sites extraprofessionnels
- Accéder à vos fichiers personnels en votre absence en cas de danger ou d'urgence pour l'entreprise
- Imposer une charte informatique à ses salariés



LE GPS DU VEHICULE DU SALARIE



L'EMPLOYEUR PEUT DÉCIDER D'INSTALLER UN GPS DANS VOTRE VÉHICULE PROFESSIONNEL, LUI PERMETTANT AINSI DE SUIVRE VOS DÉPLACEMENTS :

- **En cas de nécessité pour le suivi et la facturation des trajets aux clients**
 - **Assurer la sécurité des biens et personnes transportés**
- **Suivre le temps de travail du salarié (si aucun moyen n'existe déjà)**
- **Vérifier la conformité de l'utilisation du véhicule (au regard de la loi et de l'utilisation prévue par l'entreprise)**
 - **En cas de nécessité pour l'entreprise (UBER, réparations d'urgence etc)**

LE GPS DU VEHICULE DU SALARIE



POUR QUE CE SYSTÈME DE CONTRÔLE SOIT LICITE, L'EMPLOYEUR DOIT :

- Informer les salariés du contrôle
 - Avoir été déclaré à la CNIL

SONT INTERDITS POUR L'EMPLOYEUR

- Géolocalisation hors temps de travail
- Contrôler la vitesse du salarié en temps réel
- Géolocaliser les IRP dans l'exercice de leur mandat

LES SYSTEMES D'ECOUTE ET D'ENREGISTREMENT VOCAUX

Il est très fréquent que les entreprises mettent en place des systèmes d'écoute des conversation téléphoniques des salariés, dans plusieurs buts :

- **Contrôler la qualité du service**
- **Former les salariés**
- **Evaluer les salariés**

Toutefois, pour être légal, ce dispositif ne doit être que temporaire et ne durer que sur le temps imparti à la recherche du but poursuivi (le temps de la formation ou de l'évaluation).



LES SYSTEMES D'ECOUTE ET D'ENREGISTREMENT VOCAUX

Sauf texte imposant une durée spécifique ou justification particulière, **les enregistrements peuvent être conservés jusqu'à six mois au maximum.** Les documents d'analyse peuvent quant à eux être conservés jusqu'à un an.



Une bonne pratique : les enregistrements « tampon »

Cette pratique consiste pour l'employeur, à écouter les enregistrements dans les jours suivant leur réalisation et à rédiger le(s) document(s) d'analyse nécessaire(s). Les enregistrements sont ensuite supprimés à bref délai, l'employeur ne conservant que les documents d'analyse.

LES SYSTEMES BIOMETRIQUES

Un système biométrique, aussi appelé **Identificateur Unique Universel** est la manière la plus sûre de vérifier l'identité d'une personne puisqu'elle repose sur une caractéristique qui lui est totalement propre.

La trace biométrique la plus utilisée aujourd'hui est l'empreinte digitale, elle est utilisée pour les papiers d'identité, les permis de conduire.

Aujourd'hui, un employeur peut demander à collecter une trace biométrique de vous afin de contrôler, par exemple, votre accès aux locaux de l'entreprise.

Conservées pendant une durée de 3 mois à 5 ans, ces données qui font l'objet d'un traitement doivent être déclarées préalablement à la CNIL; faute de quoi elles ne seront opposable aux salariés.



LA VIDEOSURVEILLANCE



On peut surveiller par vidéo une rue, un couloir, un immeuble.

Mais on ne peut pas surveiller par vidéo une personne en particulier, un poste de travail, un appartement.

Les personnes susceptibles d'être enregistrées doivent être très clairement informées de ce dispositif et de leur capacité à pouvoir demander l'effacement des données collectées.

LA VIDEOSURVEILLANCE



Les images obtenues doivent être conservées 1 mois

et les systèmes doivent être déclarés à la CNIL s'il

s'agit d'un lieu privé (si la surveillance à lieu dans

l'entreprise, les institutions représentatives du

personnel doivent en avoir été informées), et à la

préfecture s'il s'agit d'un lieu public.

BYOD – Bring Your Own Device

Ce concept désigne l'usage d'équipements informatiques personnels dans un contexte professionnel.

Cet usage n'est possible que si certains critères sont remplis :

- **L'utilisation du matériel personnel ne doit être que subsidiaire :** la loi impose en effet à l'employeur de fournir au salarié les moyens nécessaires à sa fonction
- **Les données doivent rester en sécurité :** c'est à l'employeur qu'il incombe de s'assurer que les données sont en sécurité

