LSIX
LAW FIRM

DONNÉES PERSO. & CSI

Licence professionnelle Sécurité des biens et des personnes
2026 - 2027

Monsieur KARPIEL



Les données personnelles que je traite dans mon quotidien ?

Me concernant (à titre privé) : nom, adresse, n° de téléphone, e-mail, photos, géolocalisation du smartphone, données bancaires, données de santé (appli sport), historique de navigation…

Dans le cadre de mon travail (à titre professionnel dans la sécurité privée) :

- Images de vidéoprotection, enregistrements des caméras-piétons
- Registres des visiteurs, badges et journaux de contrôle d'accès
- Main courante, rapports d'incident, plaques d'immatriculation (parkings)
- Données RH des agents : plannings, cartes professionnelles CNAPS, géolocalisation des rondes
- …

Pourquoi protéger les données personnelles ?

- **Droit fondamental** : vie privée (art. 8 CEDH, art. 9 C. civ.) et protection des données (art. 7 et 8 de la Charte des droits fondamentaux de l'UE)
- **Prévenir les dérives** : surveillance de masse, fichage, profilage, discrimination (embauche, crédit, assurance)
- **Éviter les préjudices** : usurpation d'identité, escroqueries, chantage, cyberharcèlement après une fuite de données
- **Liberté** : se savoir observé conduit à l'autocensure (« effet dissuasif ») ; ce qui est anodin aujourd'hui peut être utilisé demain
- **Confiance** : condition du numérique et de l'économie ; obligation légale sanctionnée (amendes, pénal)

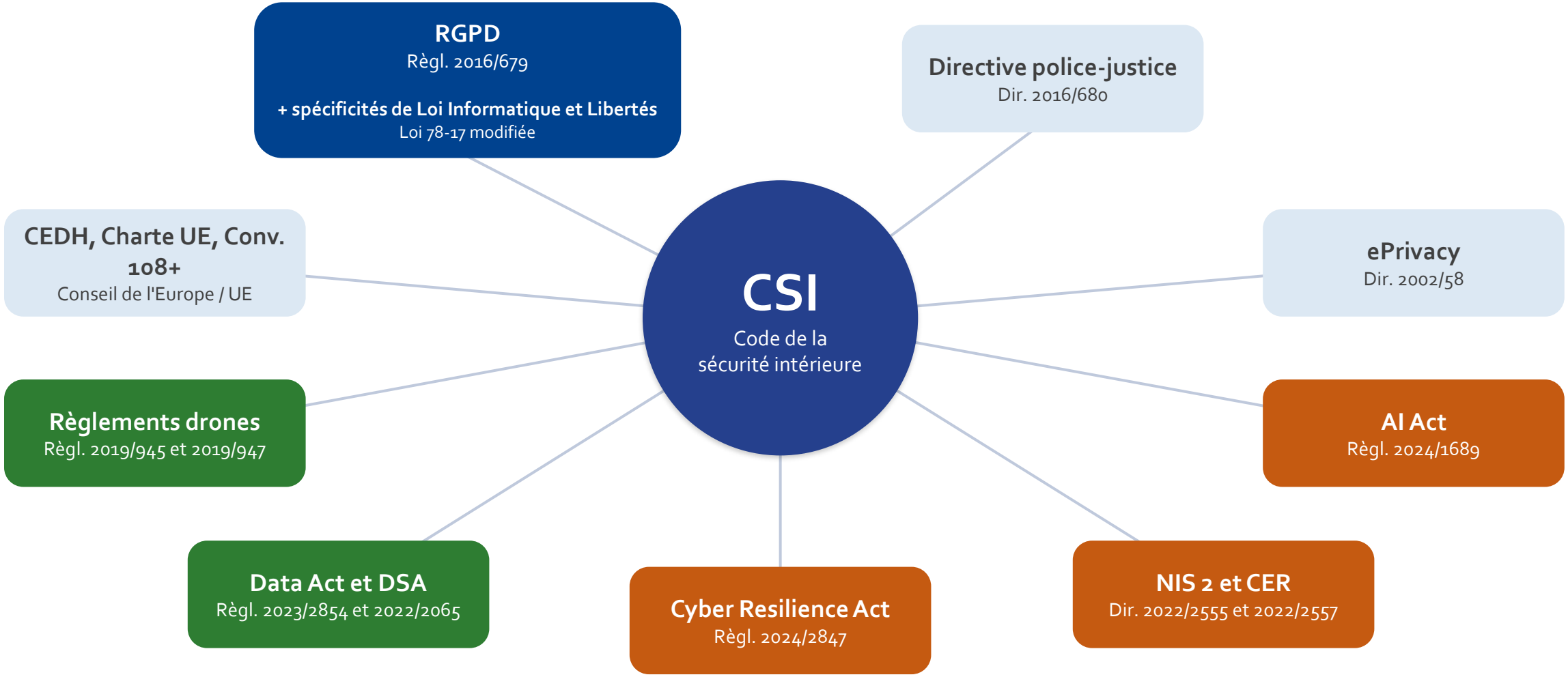
« Dire que l'on se moque de la vie privée parce que l'on n'a rien à cacher, c'est comme dire que l'on se moque de la liberté d'expression parce que l'on n'a rien à dire » (E. Snowden)

INTRODUCTION

- La France est **l'un des premiers États européens** à se doter d'une législation spécifique (après le Land de Hesse en 1970 et la Suède en 1973)

  Polémiques autour du projet **SAFARI** d'interconnexion des fichiers administratifs (Le Monde, 21 mars 1974 : « *SAFARI ou la chasse aux Français* »)
- **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés : création de la **CNIL**, autorité administrative indépendante
- **Directive 95/46/CE** du 24 octobre 1995 : premier cadre européen, transposé en 2004
- **Une évolution nécessaire ?** Oui : internet, réseaux sociaux, smartphones, cloud, big data et IA, flux mondiaux de données, géants du numérique hors UE, législations nationales disparates → **RGPD** (applicable depuis le 25 mai 2018)

Les sources de textes



Sources (1/5) : RGPD et police-justice

- **RGPD** = Règlement (UE) **2016/679** du 27 avril 2016, qui abroge la directive 95/46/CE
  - Harmonisation des législations nationales car **directement applicable** dans l'ordre interne depuis le **25 mai 2018** (sans transposition)
  - Champ : tous les traitements, organisations publiques et privées, sauf ceux relevant de la directive police-justice ou de la sûreté de l'État.
- **Directive « police-justice »** (UE) **2016/680** du 27 avril 2016 : traitements de données par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes, de poursuites, d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique
  - Transposée en droit français dans le **titre III de la loi Informatique et Libertés** (art. 87 et s.)

Sources (2/5) : le droit national

- **Loi Informatique et Libertés** n° 78-17 du 6 janvier 1978, adaptée au RGPD par la loi n° 2018-493 du 20 juin 2018, l'ordonnance n° 2018-1125 du 12 décembre 2018 et le décret n° 2019-536 du 29 mai 2019
  - elle régit seule les traitements intéressant la **sûreté de l'État** et la **défense** (titre IV) et exerce les « marges de manœuvre » du RGPD (âge du consentement numérique : 15 ans, NIR, santé…)
- **Code de la sécurité intérieure** : vidéoprotection (L. 251-1 s.), caméras-piétons (L. 241-1 s.), drones (L. 242-1 s.), activités privées de sécurité et CNAPS (livre VI)
  - modifié par les lois « **sécurité globale** » n° 2021-646 du 25 mai 2021, n° 2022-52 du 24 janvier 2022, n° 2023-380 du 19 mai 2023 (JO 2024), n° 2025-532 du 28 avril 2025 (transports) et n° **2026-201 du 20 mars 2026** (JOP 2030 : VSA prolongée)
- **Autres codes** : Code du travail (surveillance des salariés), Code pénal (art. 226-1 s.), CPCE (prospection), Code civil (art. 9)
- **Loi SREN** n° 2024-449 du 21 mai 2024 : sécurisation de l'espace numérique, renforcement des pouvoirs de l'Arcom et de la CNIL

Sources (3/5) : la directive ePrivacy

- Le 10 janvier 2017, la Commission européenne publie une proposition de règlement « **ePrivacy** »
  - Objectif : abroger la **directive 2002/58/CE du 12 juillet 2002** (« vie privée et communications électroniques ») et harmoniser les règles sur la confidentialité des communications électroniques, les cookies et la prospection
  - *« Faire en sorte que les services numériques soient plus sûrs et suscitent davantage de confiance »*
- **Mise à jour : après 8 ans de blocage au Conseil, la Commission a retiré la proposition (programme de travail 2025, février 2025).**
- La **directive 2002/58/CE** (modifiée en 2009) **reste donc applicable**, via le droit national :
  - **art. 82 de la loi Informatique et Libertés** : cookies et traceurs (consentement préalable) ;
  - **art. L. 34-5 du CPCE** : prospection par e-mail ou SMS (consentement préalable des particuliers).
- Le projet d'**omnibus numérique** (novembre 2025) propose d'intégrer une partie des règles sur les cookies dans le RGPD : à suivre

Sources (4/5) : IA et cybersécurité

Règlement IA (AI Act) – (UE) 2024/1689

- En vigueur le 1er août 2024 ; interdictions depuis le **2 février 2025** (reconnaissance faciale en temps réel, émotions au travail…)
- Systèmes **biométriques** et de sécurité = **haut risque** : obligations reportées par l'omnibus numérique
- Sanctions jusqu'à **35 M€ ou 7 %** du CA mondial ; CNIL autorité de contrôle

Directive NIS 2 – (UE) 2022/2555

- **Cybersécurité** de milliers d'entités « essentielles » et « importantes » (énergie, transports, santé, numérique…)
- Gestion des risques, signalement des incidents à l'ANSSI, responsabilité des dirigeants
- Transposition française : loi « résilience » (2025-2026)

Directive CER – (UE) 2022/2557

- **Résilience des entités critiques** : protection **physique** des sites, contrôle des accès, **vérification des antécédents** du personnel sensible
- Remplace la directive 2008/114 ; s'articule avec le dispositif français des opérateurs d'importance vitale (OIV)
- Directement lié aux missions de sûreté et de sécurité privée

Cyber Resilience Act – (UE) 2024/2847

- Exigences de **cybersécurité des produits connectés** : caméras IP, enregistreurs, contrôle d'accès, objets connectés
- Signalement des vulnérabilités exploitées à partir du **11 septembre 2026**
- Application complète le **11 décembre 2027** (marquage CE)

Sources (5/5) : données, plateformes, drones

Data Act – (UE) 2023/2854

- Applicable depuis le **12 septembre 2025**
- Accès et partage des **données générées par les objets connectés** (dont caméras et capteurs) ; s'applique sans préjudice du RGPD

Digital Services Act – (UE) 2022/2065

- Applicable à toutes les plateformes depuis le **17 février 2024**
- Signalement et retrait des **contenus illicites** : ex. vidéo de surveillance diffusée sur un réseau social ; en France, Arcom (loi SREN)

Règlements drones – (UE) 2019/945 et 2019/947

- Catégories ouverte / spécifique / certifiée, enregistrement des exploitants, formation des télépilotes
- Complétés par le droit national (loi n° 2016-1428, signalement électronique) et le CSI pour les forces de l'ordre

Conseil de l'Europe et droits fondamentaux

- **CEDH** (art. 8) et **Charte des droits fondamentaux** de l'UE (art. 7 et 8)
- **Convention 108** modernisée (« 108+ », 2018) ; **convention-cadre sur l'IA** ouverte à la signature le 5 septembre 2024

Synthèse : qui fait quoi ?

Texte	Objet principal	Exemple pour la sécurité privée	Applicable
RGPD (2016/679)	Tous les traitements de données	Registre, information, droits, AIPD, sous-traitance	25 mai 2018
Loi I&L / CSI	Règles françaises, vidéoprotection	Autorisation préfectorale, 1 mois de conservation	1978 / 2012
Directive police-justice	Police, justice	Transmission d'images sur réquisition	2018
ePrivacy (2002/58)	Communications, cookies	Site web de l'entreprise, prospection	2002 (2009)
AI Act (2024/1689)	Systèmes d'IA	Caméras augmentées, biométrie	2025 → 2027
NIS 2 / CER	Cyber / résilience des sites	Sûreté des sites critiques, antécédents	Transposition 2025-26
Cyber Resilience Act	Produits connectés	Caméras IP sécurisées	2026 → 2027
Data Act / DSA	Données IoT / plateformes	Données des capteurs ; vidéos en ligne	2025 / 2024
Règl. drones 2019/947	Aviation civile	Surveillance de site par drone	2021

DEFINITION : Donnée personnelle

Toute information se rapportant à une personne physique **identifiée ou identifiable** (art. 4.1 RGPD) :

- **Directement**
  - nom, prénom, photographie du visage

- **Indirectement**
  - adresse postale, n° de téléphone, adresse e-mail, n° de sécurité sociale (NIR), plaque d'immatriculation, adresse IP, identifiant de connexion, n° de badge, empreinte digitale, données de géolocalisation…

DEFINITION : Donnée personnelle

Toute information se rapportant à une personne physique **identifiable** :

- **à partir d'une seule donnée**
  - n° de sécurité sociale, n° de téléphone mobile, ADN, empreinte digitale, adresse e-mail nominative (prenom.nom@…)
- **à partir du croisement d'un ensemble de données**
  - ex. : « femme, 35 ans, cheffe de poste chez tel prestataire, habitant telle commune, garée chaque soir sur le parking P2 » permet de retrouver une seule personne

Des données pseudonymisées restent des données personnelles ; seules les données réellement anonymisées (ré-identification impossible) sortent du RGPD (considérant 26).

DEFINITION : Traitement de données personnelles

Opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (*collecte, enregistrement, organisation, structuration, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement, limitation, effacement ou destruction*) – art. 4.2 RGPD

❖ **Exemples**

- **Tenue d'un fichier des mains courantes** du poste de sécurité, d'un registre des visiteurs, d'une liste de badges
- **Collecte** : relevé de l'identité d'un visiteur à l'accueil, enregistrement des images d'une caméra
- **Mise à jour** : désactivation du badge d'un salarié parti, correction d'une erreur dans un rapport

Informatisé ou papier ? Les deux : le RGPD s'applique aussi aux fichiers papier structurés (art. 2.1).

DEFINITION : Traitement de données personnelles

- Doit avoir un objectif, une **finalité** déterminée, explicite et légitime
- Doit reposer sur une **base légale** (art. 6) et être **proportionné** au regard de votre activité professionnelle

Interdiction de principe (sauf exceptions limitées) de collecter ou traiter :

- les **données sensibles** (art. 9) : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, **biométriques** (identification), de **santé**, vie et orientation sexuelles
- les **données relatives aux condamnations et infractions** (art. 10 RGPD, art. 46 loi I&L) : réservées aux autorités publiques, auxiliaires de justice, victimes pour se défendre…
- le **NIR** (n° de sécurité sociale) en dehors des cas prévus par décret
- des données **non pertinentes ou excessives**, ou collectées de façon **déloyale** (à l'insu des personnes)

Exceptions possibles : consentement explicite, obligations en droit du travail, intérêt vital, données rendues publiques par la personne, défense en justice, intérêt public important…

DEFINITION : Traitement de données personnelles

Exemple : dans l'entreprise CONFORME_DP, un service s'occupe de la paie.

- **Finalité principale** : gestion de la paie et de la rémunération des salariés

❖ **Sous-finalité 1** : calcul des salaires, primes, heures supplémentaires et retenues

❖ **Sous-finalité 2** : établissement et remise des bulletins de paie

❖ **Sous-finalité 3** : déclarations sociales et fiscales obligatoires (DSN, prélèvement à la source)

❖ **Sous-finalité 4** : gestion des congés, absences et arrêts maladie ayant un impact sur la paie

→ *Chaque sous-finalité doit être compatible avec la finalité principale ; les données de paie ne peuvent pas être réutilisées, par exemple, pour de la prospection.*

DEFINITION : Responsable de traitement

- Celui qui **détermine les finalités et les moyens** du traitement (art. 4.7 RGPD)
- Il décide du « **pourquoi** » et du « **comment** » les données sont traitées

Il a des obligations (principe de responsabilité – « accountability », art. 5.2 et 24) :

- tenir le **registre** des activités de traitement (art. 30)
- **informer** les personnes et leur permettre d'exercer leurs **droits** (art. 12 à 22)
- assurer la **sécurité** des données (art. 32) et la protection dès la conception (art. 25)
- encadrer ses **sous-traitants** par contrat (art. 28)
- réaliser une **analyse d'impact (AIPD)** pour les traitements à risque élevé (art. 35)
- **notifier les violations** à la CNIL sous 72 h (art. 33) et informer les personnes si risque élevé (art. 34)
- désigner un **DPO** lorsque c'est obligatoire (art. 37) et coopérer avec la CNIL

Le registre des traitements (art. 30)

Le registre du responsable de traitement contient :

- nom et coordonnées du responsable, de son représentant et du **DPO**
- les **finalités** du traitement
- les catégories de **personnes concernées** et de **données**
- les catégories de **destinataires**, y compris hors UE
- les **transferts** vers un pays tiers et leurs garanties
- si possible, les **délais d'effacement**
- si possible, une description des **mesures de sécurité** (art. 32)

Ce qu'il faut retenir

- Le **sous-traitant** tient aussi un registre des traitements qu'il effectue pour ses clients (art. 30.2) : c'est le cas d'une entreprise de sécurité privée qui assure la vidéosurveillance ou le contrôle d'accès pour le compte d'une entreprise cliente. À retenir : une même entreprise peut être à la fois responsable de traitement (pour ses propres données RH, par exemple) et sous-traitante (pour les données traitées pour ses clients).
- Registre **écrit**, papier ou électronique (art. 30.3)
- Mis à la **disposition de la CNIL** sur demande (art. 30.4)
- Exemption pour les organismes de **moins de 250 salariés**. **Pas d'exemption si : traitement non occasionnel, à risque ou portant sur des données sensibles ou d'infraction** (art. 30.5).

  En pratique, registre presque toujours obligatoire (paie, vidéo…)

Registre : exemple de fiche

Rubrique du registre (art. 30)	Vidéoprotection d'un magasin
Responsable du traitement / DPO	SAS MAGASIN CONFORME – DPO : dpo@conforme.fr
Finalité(s)	Sécurité des personnes et des biens, prévention des vols et agressions
Base légale	Intérêt légitime (art. 6.1.f) + autorisation préfectorale (CSI, L. 252-1)
Personnes concernées	Clients, visiteurs, salariés, prestataires
Catégories de données	Images (date, heure, lieu) ; pas de son, pas de biométrie
Destinataires	Agents autorisés du sous-traitant ; forces de l'ordre sur réquisition
Sous-traitant	Société de sécurité privée (contrat art. 28), hébergeur des enregistrements
Transferts hors UE	Aucun
Durée de conservation	30 jours, puis effacement automatique
Mesures de sécurité	Accès nominatifs, journalisation, écran hors de la vue du public, chiffrement

I. RGPD

I.1. Périmètre du RGPD?

S'applique à toute organisation, publique ou privée, qui traite des données personnelles **pour son compte ou pour le compte d'autrui** (sous-traitant), dès lors (art. 3) :

- qu'elle est **établie** sur le territoire de l'Union européenne (même si le traitement a lieu ailleurs),
- ou que son activité **cible** des personnes qui se trouvent dans l'UE (offre de biens ou services, …).

Exemples :

- une société française de sécurité privée qui stocke ses plannings sur un serveur au Maroc → RGPD applicable (établissement principal en UE)
- un site américain qui vend en euros et livre en France → RGPD applicable (vend des biens ou services)
- une application étrangère qui géolocalise des utilisateurs en Europe → RGPD applicable (suivi du comportement)

Exclus : usage strictement personnel ou domestique (carnet d'adresses privé), traitements de la police (directive 2016/680) et de la défense nationale

I.2. Les grands principes du RGPD

Principe de finalité (art. 5.1.b RGPD)

Le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but **déterminé, explicite et légitime**.

Ce principe limite la manière dont le responsable peut utiliser ou **réutiliser** ces données dans le futur : une finalité ultérieure n'est permise que si elle est **compatible** avec la finalité initiale (art. 6.4 : lien entre les finalités, contexte, attentes raisonnables des personnes, garanties).

Exemples de finalités : gestion des recrutements, gestion de la paie, gestion des clients, enquête de satisfaction, sécurité des locaux (vidéoprotection), contrôle d'accès.

Ex. de détournement : utiliser les images de vidéoprotection pour surveiller la productivité des salariés.

I.2. Les grands principes du RGPD

Principe de minimisation : proportionnalité et pertinence (art. 5.1.c)

Les données doivent être **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard de la finalité.

Exemples de données non pertinentes ou excessives :

- la situation professionnelle de l'entourage d'un candidat dans un fichier de recrutement
- le numéro de carte d'identité pour délivrer un extrait d'acte d'état civil
- le numéro de sécurité sociale pour l'inscription à l'école ou aux activités périscolaires
- une copie de la pièce d'identité de chaque visiteur conservée à l'accueil d'un site (un relevé du nom suffit en général – sauf si règlementation spécifique site sensible)

Attention aux champs libres et aux zones de commentaires (ex. : main courante) : pas de propos subjectifs, insultants ou relatifs à la santé ou aux opinions.

I.2. Les grands principes du RGPD

Principe de limitation de la conservation (art. 5.1.e)

Il n'est pas possible de conserver des informations sur des personnes physiques pour une durée indéfinie. Une **durée précise** doit être fixée, en fonction du type d'information et de la finalité, puis les données sont **supprimées ou anonymisées**.

Le cycle de vie de la donnée en 4 phases (diapos suivantes) :

- 1. Conservation en **base active**
- 2. **Archivage intermédiaire (si nécessaire)**
- 3. **Archivage définitif (si nécessaire)**
- 4. **Destruction**

I.2. Les grands principes du RGPD

Le cycle de vie de la donnée – 1. Conservation en base active

C'est la durée **nécessaire à la réalisation de l'objectif** (finalité) ayant justifié la collecte. Les données sont accessibles aux services opérationnels.

Exemples :

- les données d'un **candidat non retenu** peuvent être conservées **2 ans maximum** après le dernier contact, s'il en est informé et ne s'y oppose pas (référentiel CNIL)
- les **images de vidéoprotection** : quelques jours, **1 mois maximum**
- les données d'un **client** : pendant toute la relation commerciale

I.2. Les grands principes du RGPD

Le cycle de vie de la donnée – 2. Archivage intermédiaire (si nécessaire)

Les données ne sont plus utilisées pour atteindre l'objectif fixé (« dossiers clos ») mais présentent encore un **intérêt administratif** (gestion d'un éventuel contentieux, délais de prescription) ou doivent être conservées pour répondre à une **obligation légale**.

- ex. : les pièces comptables et factures sont conservées **10 ans** (C. com., L. 123-22), même si la personne n'est plus cliente
- ex. : les images de vidéoprotection extraites pour une procédure judiciaire sont conservées jusqu'à son terme

Les données sont alors placées dans une **base distincte** ou isolées logiquement, et consultées de manière ponctuelle et motivée par des **personnes spécifiquement habilitées**.

I.2. Les grands principes du RGPD

Le cycle de vie de la donnée – 3. Archivage définitif (si nécessaire)

En raison de leur « valeur » et de leur intérêt (historique, scientifique, statistique), certaines informations sont archivées de manière **définitive et pérenne**, dans les conditions du Code du patrimoine.

À la différence de la conservation en base active, les deux dernières étapes ne sont **pas systématiques**. Leur nécessité doit être évaluée pour chaque traitement et, pour chacune de ces phases, un **tri** doit être opéré entre les données.

Le cycle de vie de la donnée – 4. Destruction

I.2. Exemples de durées de conservation

Données	Durée	Source
Images de vidéoprotection	1 mois maximum	CSI, L. 252-5 ; CNIL
Journaux de badges / contrôle d'accès	3 mois	CNIL
Géolocalisation d'un véhicule de service	2 mois (1 an pour l'optimisation des tournées)	CNIL
Candidat non retenu	2 ans après le dernier contact	Référentiel CNIL recrutement
Bulletins de paie (copie employeur)	5 ans	C. trav., L. 3243-4
Clients / prospects (prospection)	3 ans après le dernier contact	Référentiel CNIL
Pièces comptables, factures	10 ans	C. com., L. 123-22
Consentement aux cookies	6 mois recommandés ; traceurs 13 mois max	CNIL
Journaux de connexion (logs)	6 mois à 1 an	Recommandation CNIL

Les anciennes « normes simplifiées » (NS-048…) ont disparu en 2018 ; voir les référentiels CNIL, dont le référentiel RH de durées de conservation (avril 2026).

I.2. Les grands principes du RGPD

Principe de sécurité et de confidentialité (art. 5.1.f et 32) : le responsable doit garantir la sécurité et la confidentialité des données qu'il détient, en fonction des risques.

- seules les **personnes autorisées** accèdent aux données (habilitations, mots de passe robustes, authentification multifacteur)
- **traçabilité** des accès, sauvegardes, chiffrement, mises à jour
- sécurité **physique** (locaux, PC sécurité, écrans)
- encadrement des **sous-traitants**

Référence : « Guide de la sécurité des données personnelles » de la CNIL (édition 2024)



I.2. Les grands principes du RGPD

Exercice : dispositif biométrique (empreinte digitale) de pointage des heures de travail dans un commerce alimentaire

- **Finalité** : contrôle des horaires de travail : légitime en soi, mais n'exige pas d'identifier les salariés par leur corps
- **Proportionnalité et pertinence** : **disproportionné** ; la biométrie (donnée sensible, art. 9) est réservée au contrôle d'accès à des locaux, appareils ou applications sensibles (règlement type CNIL de 2019) → badge, code ou feuille d'émargement suffisent
- **Durée de conservation limitée** : gabarits supprimés au départ du salarié ; relevés d'horaires conservés 1 an (C. trav., D. 3171-16)
- **Confidentialité** : accès réservé au service RH ; information individuelle des salariés, consultation du CSE
- **Sécurité** : à défaut d'alternative, gabarit stocké sur un support détenu par le salarié (badge / selon technologie), chiffrement, pas de base centrale

Conclusion : si aucune justification valable alors illicite ; la CNIL a déjà sanctionné des employeurs pour ce type de pointeuse.

I.2. Les grands principes du RGPD

Les droits des personnes (développés dans les diapos suivantes)

Les personnes concernées disposent de droits leur permettant de **garder la maîtrise** des informations les concernant (art. 12 à 22 RGPD).

Le responsable doit leur expliquer la procédure (où, comment et à qui s'adresser ?) permettant de les **exercer concrètement**, et faciliter cet exercice.

Délai de réponse : 1 mois, prolongeable de 2 mois en cas de demandes complexes ou nombreuses, à condition d'en informer la personne dans le premier mois (art. 12.3).

L'exercice des droits est en principe **gratuit**.

I.3. RGPD et DROITS des personnes

RÉCAPITULATIF DES NOUVEAUX DROITS

Intitulé	Définition	Complexité
droit d'accès	demander la confirmation ou infirmation que ses données font l'objet d'un traitement, et en demander l'accès (dont types de traitement et finalités)	moyenne
droit de rectification	demander la rectification de ses données	moyenne
droit à l'effacement	demander l'effacement de ses données dans les meilleurs délais	faible
droit à la limitation du traitement	demander la limitation du traitement de ses données (ou le non-effacement)	moyenne
droit à la portabilité des données	recevoir sur demande ses données personnelles dans un format structuré, utilisé et lisible pour le transmettre éventuellement à un nouveau responsable de traitement	forte
droit d'opposition	s'opposer au traitement de ses données (dont profilage)	faible
droit au refus d'une décision sur traitement automatisé	refuser de faire l'objet d'une prise de décision fondée uniquement sur un traitement automatisé	moyenne
droit d'informations de collectes et traitements de données	être informé de la collecte, conservation, et exploitation de ses données pour une finalité précise	forte

I.3. RGPD et DROITS des personnes

Le droit à l'information (art. 13 et 14 RGPD)

Pour être loyale et licite, la collecte doit s'accompagner d'une information **concise, transparente, compréhensible et aisément accessible** sur :

- l'identité et les coordonnées du responsable et, le cas échéant, du **DPO** ;
- les **finalités** et la **base légale** du traitement (et l'intérêt légitime poursuivi s'il en est la base) ;
- le caractère obligatoire ou facultatif des réponses et les conséquences d'un défaut de réponse ;
- les **destinataires** et les éventuels **transferts hors UE** ;
- la **durée de conservation** ;
- les **droits** : accès, rectification, effacement, limitation, opposition, portabilité, retrait du consentement, directives post-mortem ;
- le droit d'introduire une **réclamation auprès de la CNIL** ;
- l'existence d'une **décision automatisée** ou d'un profilage.

I.3. RGPD et DROITS des personnes

Le droit d'opposition (art. 21 RGPD)

- **Prospection commerciale** : droit **absolu**, sans motif à donner. Le choix doit être proposé dès la collecte (case à cocher non pré-cochée) ; une simple mention dans les CGV ne suffit pas. Par e-mail ou SMS, le **consentement préalable** des particuliers est requis (CPCE, L. 34-5).
- **Autres traitements** : toute personne peut s'opposer pour des **raisons tenant à sa situation particulière** lorsque le traitement repose sur l'**intérêt légitime** ou une **mission d'intérêt public** ; le responsable doit cesser, sauf **motifs légitimes et impérieux** ou défense en justice.
- **Pas de droit d'opposition** lorsque le traitement repose sur une **obligation légale** (ex. : fichiers des impôts) ou sur l'exécution d'un **contrat**.
- Le **consentement**, lui, peut être **retiré** à tout moment (art. 7.3).

I.3. RGPD et DROITS des personnes

Les droits d'accès (art. 15) et de rectification (art. 16)

Toute personne peut :

- obtenir la **confirmation** que des données la concernant sont traitées et y **accéder** ;
- connaître les finalités, les destinataires, la **durée de conservation** et l'**origine** des données ;
- accéder aux informations sur lesquelles le responsable s'est fondé pour prendre une décision la concernant (ex. : éléments ayant conduit au refus d'une promotion, score bancaire ayant motivé le rejet d'un crédit) ;
- en obtenir **une copie gratuite** ; seules les copies supplémentaires peuvent donner lieu à des frais raisonnables ;
- exiger que ses données inexactes soient **rectifiées** ou complétées ;
- et, selon les cas, demander leur **effacement** (art. 17), la **limitation** du traitement (art. 18) ou leur **portabilité** (art. 20).

I.3. RGPD et DROITS des personnes

Exercer ses droits d'accès et de rectification

- **Par écrit** : courrier postal ou **voie électronique** (formulaire, e-mail au DPO). Un justificatif d'identité ne peut être demandé qu'en cas de **doute raisonnable** sur l'identité du demandeur.
- **Sur place** : il est possible de se faire accompagner par la personne de son choix ; la consultation doit permettre de prendre note commodément et complètement ; une copie peut être demandée.
- **Délai** : 1 mois à compter de la réception de la demande, prolongeable de 2 mois si nécessaire (la personne doit en être informée).
- **Vidéoprotection** : droit d'accès spécifique aux enregistrements (CSI, L. 252-3) ; les tiers visibles doivent être floutés.
- **En cas de refus ou d'absence de réponse** : réclamation auprès de la CNIL.

I.3. RGPD et DROITS des personnes

Les limites au droit d'accès

- Demandes **manifestement infondées ou excessives**, notamment répétitives : refus ou frais raisonnables, à justifier (art. 12.5)
- **Droits des tiers** : la copie ne doit pas porter atteinte aux droits et libertés d'autrui (art. 15.4) : floutage des autres personnes, secret des affaires
- **Données anonymisées** ou dont le responsable ne peut plus identifier la personne (art. 11)
- **Fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique** : **droit d'accès indirect** exercé par l'intermédiaire de la CNIL (ex. fichiers de renseignement)
- **Fichiers de police judiciaire** (TAJ…) : accès selon les règles propres à la directive police-justice
- Limitations prévues par la loi au titre de l'**art. 23 RGPD** (enquêtes, secret professionnel…)

I.4. Bases de traitements

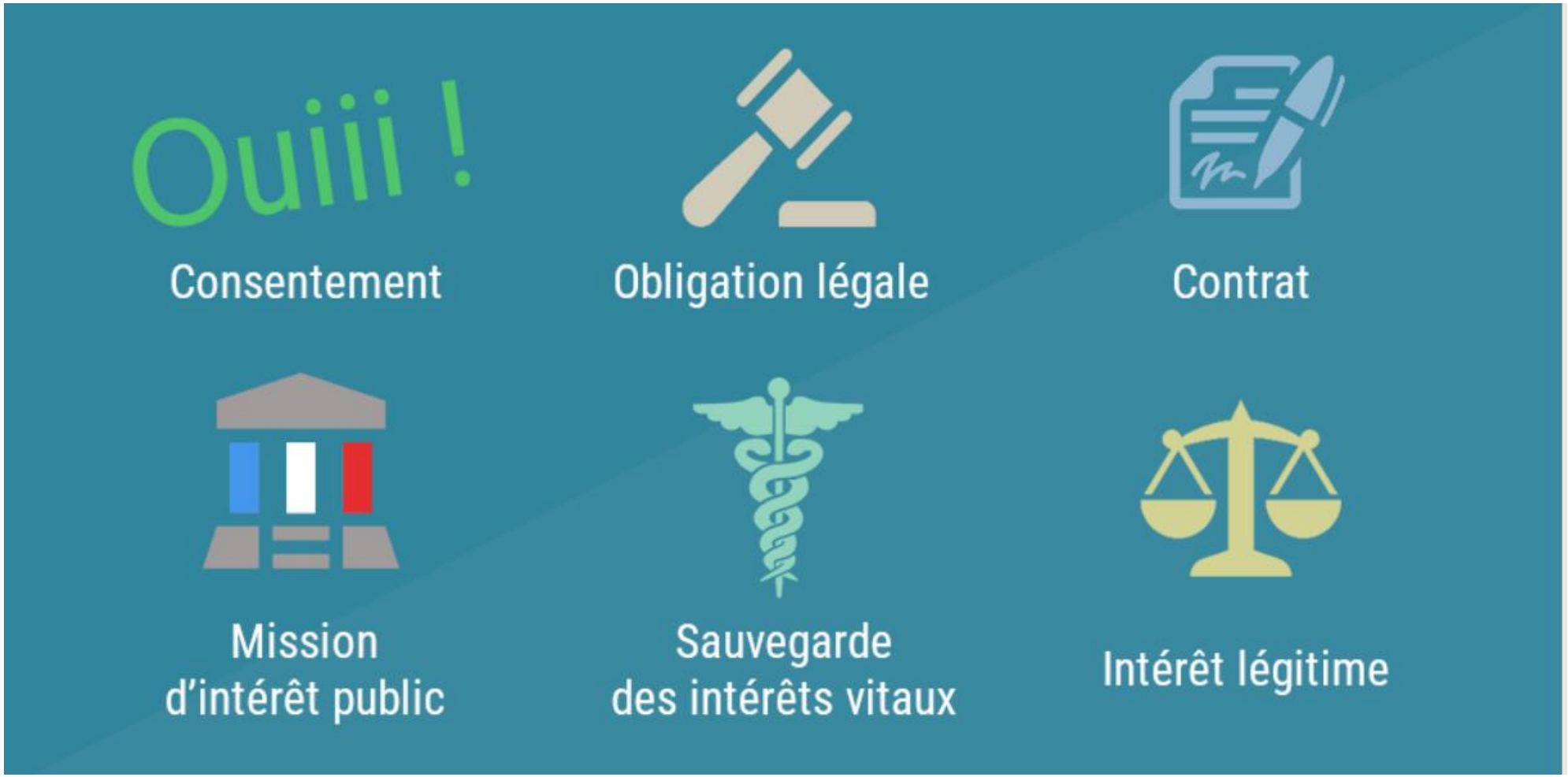
La **base légale** d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de collecter ou d'utiliser des données personnelles (art. 6 RGPD). On parle aussi de « fondement juridique ».

Six bases légales sont prévues par le RGPD :

- le **consentement** ;
- le **contrat** ;
- l'**obligation légale** ;
- la sauvegarde des **intérêts vitaux** ;
- la **mission d'intérêt public** ;
- les **intérêts légitimes**.

*Une seule base par finalité, choisie **avant** la mise en œuvre et indiquée dans l'information des personnes. Il n'y a pas de hiérarchie entre elles.*

I.4. Bases de traitements



I.4. Bases de traitements

La base contractuelle (art. 6.1.b)

Le traitement doit être **objectivement nécessaire** à l'exécution d'un contrat conclu avec la personne concernée, ou à des mesures précontractuelles prises à sa demande.

- ex. : gestion des données d'un client pour livrer sa commande ; paie d'un salarié (en lien avec le contrat de travail)
- contre-ex. : la prospection commerciale ou la vidéoprotection ne sont pas nécessaires à l'exécution du contrat

I.4. Bases de traitements

Le consentement (art. 4.11 et 7 RGPD)

- Manifestation de volonté **libre, spécifique, éclairée et univoque**, par une déclaration ou un **acte positif clair** (case non pré-cochée, clic) ; il doit être recueilli **avant** la collecte
- Le responsable doit pouvoir **prouver** le consentement ; il peut être **retiré** à tout moment, aussi simplement qu'il a été donné
- Rarement libre dans la **relation de travail** (déséquilibre) : à éviter comme base légale vis-à-vis des salariés

Il est notamment requis :

- pour les **données sensibles** (consentement **explicite**, art. 9.2.a) ;
- pour les **cookies et traceurs** non essentiels (art. 82 loi I&L) ;
- pour la **prospection par voie électronique** auprès des particuliers (CPCE, L. 34-5) ;
- pour les mineurs de moins de **15 ans** en ligne : consentement conjoint du titulaire de l'autorité parentale.

I.4. Bases de traitements

L'obligation légale (art. 6.1.c)

Le traitement est **imposé** à l'organisme par un texte du droit de l'UE ou du droit français, qui en fixe la finalité.

- ex. : déclarations sociales (DSN), registre unique du personnel, conservation des factures
- ex. : enquête administrative préalable sur les agents de sécurité privée et carte professionnelle délivrée par le CNAPS
- Pas de droit d'opposition ni de droit à la portabilité sur cette base

I.4. Bases de traitements

La mission d'intérêt public (art. 6.1.e)

Le traitement est nécessaire à l'exécution d'une **mission d'intérêt public** ou relevant de l'**exercice de l'autorité publique**. Elle concerne surtout les autorités publiques, mais aussi des organismes privés chargés d'une mission de service public.

- ex. : vidéoprotection de la voie publique par une commune, gestion de la cantine scolaire
- **Les autorités publiques ne peuvent pas invoquer l'intérêt légitime pour leurs missions (art. 6.1, dernier alinéa).**

I.4. Bases de traitements

L'intérêt légitime (art. 6.1.f)

Le traitement est nécessaire aux intérêts légitimes de l'organisme (commerciaux, sécurité des biens et des personnes, prévention de la fraude…), **à condition** que ne prévalent pas les intérêts et droits fondamentaux des personnes.

- ex. : **vidéoprotection d'un magasin**, contrôle d'accès aux locaux, prévention de la fraude
- Le responsable doit **documenter la mise en balance** : intérêt réel et légitime, nécessité, attentes raisonnables des personnes
- Les personnes disposent d'un **droit d'opposition** (art. 21)

I.4. Bases de traitements

Exercice GROUPE 1

Base d'utilisation **limitée** : il faut démontrer qu'un intérêt vital est en jeu et que le traitement est nécessaire pour le sauvegarder. Le considérant 46 vise un « **intérêt essentiel à la vie** » de la personne concernée ou d'une autre personne physique.

- ex. : une victime d'accident, inconsciente, admise à l'hôpital et incapable de consentir
- ex. : un agent de sécurité qui transmet aux secours l'identité et l'état d'une personne en malaise
- contre-ex. : un traitement médical planifié ne relève pas de cette base

Elle ne doit être utilisée que si aucune autre base n'est applicable.

I.4. Bases de traitements

La sauvegarde des intérêts vitaux (art. 6.1.d)

Base d'utilisation **limitée** : il faut démontrer qu'un intérêt vital est en jeu et que le traitement est nécessaire pour le sauvegarder. Le considérant 46 vise un « **intérêt essentiel à la vie** » de la personne concernée ou d'une autre personne physique.

- ex. : une victime d'accident, inconsciente, admise à l'hôpital et incapable de consentir
- ex. : un agent de sécurité qui transmet aux secours l'identité et l'état d'une personne en malaise
- contre-ex. : un traitement médical planifié ne relève pas de cette base

Elle ne doit être utilisée que si aucune autre base n'est applicable.

Exercice : déterminer les bonnes finalités

Consignes

- La classe est répartie en **6 groupes** ; chaque groupe reçoit une diapo de **10 situations** différentes
- Pour chaque situation, indiquez la **finalité** du traitement : pourquoi les données sont-elles collectées ?
- Proposez la **base légale** (art. 6 RGPD)
- Précisez si cette finalité est **légitime**, et repérez les **détournements** et les traitements **interdits**
- Durée : 15 minutes, puis restitution orale par groupe

Les lieux rencontrés dans les situations

A	Centre commercial
B	Entreprise de sécurité
C	Copropriété
D	Clinique
E	Stade
F	Entrepôt logistique

CSI & données personnelles

Exercices

Groupe 1

Pour chacune des 10 situations, indiquez la **finalité** du traitement de données et précisez si elle est **légitime**.

N°	Situation (lieu : traitement de données)	Finalité | Base légale | Point d'attention
1	**Centre commercial** : caméras filmant les entrées, les allées et le parking clients	
2	**Entreprise de sécurité** : plannings et affectation des agents sur les sites	
3	**Copropriété** : caméras dans le hall et le parking souterrain	
4	**Clinique** : dossier médical du patient	
5	**Stade** : reconnaissance faciale à l'entrée pour repérer les interdits de stade	
6	**Entrepôt logistique** : géolocalisation des chariots élévateurs	
7	**Centre commercial** : caméra augmentée aux caisses automatiques du supermarché	
8	**Entreprise de sécurité** : arrêts de travail des agents conservés dans leur dossier	
9	**Copropriété** : coordonnées des copropriétaires transmises à une agence immobilière partenaire	
10	**Clinique** : liste de patients célèbres transmise à la presse par un agent	

Groupe 2

Pour chacune des 10 situations, indiquez la **finalité** du traitement de données et précisez si elle est **légitime**.

N°	Situation (lieu : traitement de données)	Finalité | Base légale | Point d'attention
1	**Entreprise de sécurité** : copie de la carte professionnelle CNAPS de chaque agent	
2	**Copropriété** : appels de fonds et relances des impayés	
3	**Clinique** : bouton d'alerte sonore au guichet des urgences	
4	**Stade** : caméras augmentées détectant les mouvements de foule	
5	**Entrepôt logistique** : scanners mesurant chaque seconde d'inactivité des préparateurs	
6	**Centre commercial** : fichier des « voleurs connus » partagé entre toutes les enseignes	
7	**Entreprise de sécurité** : enquête de satisfaction auprès des clients donneurs d'ordre	
8	**Copropriété** : feuille de présence et votes en assemblée générale	
9	**Clinique** : journaux d'accès au dossier patient informatisé	
10	**Stade** : images transmises en direct au PC des forces de l'ordre	

Groupe 3

Pour chacune des 10 situations, indiquez la **finalité** du traitement de données et précisez si elle est **légitime**.

N°	Situation (lieu : traitement de données)	Finalité | Base légale | Point d'attention
1	**Copropriété** : fichier des copropriétaires (nom, adresse, lots, tantièmes)	
2	**Clinique** : caméras dans la salle d'attente des urgences	
3	**Stade** : caméras de vidéoprotection dans les tribunes	
4	**Entrepôt logistique** : empreinte digitale pour entrer dans la salle des serveurs	
5	**Centre commercial** : capteurs de comptage des visiteurs aux portes	
6	**Entreprise de sécurité** : bulletin n° 3 du casier judiciaire exigé de tous les candidats	
7	**Copropriété** : liste des occupants et de leurs téléphones remise au gardien	
8	**Clinique** : vidéo des couloirs utilisée pour évaluer les infirmières	
9	**Stade** : enregistrement des interventions du poste de secours	
10	**Entrepôt logistique** : vidéo d'un salarié pris en train de voler diffusée sur WhatsApp	

Groupe 4

Pour chacune des 10 situations, indiquez la **finalité** du traitement de données et précisez si elle est **légitime**.

N°	Situation (lieu : traitement de données)	Finalité | Base légale | Point d'attention
1	**Clinique** : enregistrement des visiteurs à l'accueil (nom, chambre visitée)	
2	**Stade** : liste des supporters exclus pour non-respect des conditions de vente	
3	**Entrepôt logistique** : caméras dans les zones de stockage	
4	**Centre commercial** : relevé de l'identité d'une personne interpellée pour vol, en attendant la police	
5	**Entreprise de sécurité** : suivi des formations (MAC, SST, SSIAP)	
6	**Copropriété** : transmission des images à la police en cas d'atteinte grave dans le hall	
7	**Clinique** : registre des incidents de violence	
8	**Stade** : fichier des spectateurs pour la newsletter du club	
9	**Entrepôt logistique** : caméra-piéton de l'agent de sécurité lors des contrôles de sortie	
10	**Centre commercial** : utiliser les images pour vérifier les horaires d'arrivée des vendeurs	

Groupe 5

Pour chacune des 10 situations, indiquez la **finalité** du traitement de données et précisez si elle est **légitime**.

N°	Situation (lieu : traitement de données)	Finalité | Base légale | Point d'attention
1	**Stade** : billetterie nominative	
2	**Entrepôt logistique** : registre des visiteurs et des transporteurs	
3	**Centre commercial** : main courante électronique du PC sécurité	
4	**Entreprise de sécurité** : bulletins de paie	
5	**Copropriété** : extranet de la copropriété	
6	**Clinique** : bracelets géolocalisés pour des patients désorientés	
7	**Stade** : drone du prestataire survolant le parvis et les rues voisines	
8	**Entrepôt logistique** : données des intérimaires transmises par l'agence d'intérim	
9	**Centre commercial** : formulaire de déclaration des objets trouvés	
10	**Entreprise de sécurité** : géolocalisation des véhicules utilisée pour sanctionner les excès de vitesse	

Groupe 6

Pour chacune des 10 situations, indiquez la **finalité** du traitement de données et précisez si elle est **légitime**.

N°	Situation (lieu : traitement de données)	Finalité | Base légale | Point d'attention
1	**Entrepôt logistique** : lecture automatisée des plaques des camions (LAPI) à l'entrée	
2	**Centre commercial** : registre des clés et badges remis aux agents de sécurité	
3	**Entreprise de sécurité** : dispositif PTI/DATI géolocalisé pour les agents en ronde isolée	
4	**Copropriété** : badges d'accès au parking	
5	**Clinique** : badges d'accès à la pharmacie interne	
6	**Stade** : accréditations des stadiers et prestataires (photo, identité)	
7	**Entrepôt logistique** : alcootest avant la prise de poste des caristes	
8	**Centre commercial** : enregistrement des appels reçus au numéro d'urgence du PC sécurité	
9	**Entreprise de sécurité** : photos des agents publiées sur le site internet de l'entreprise	
10	**Copropriété** : photo d'un résident accusé de dégradations affichée dans le hall	

Corrections

Exercice sur les finalités – éléments de réponse

II. SANCTIONS